



# *University of* **HUDDERSFIELD**

## **University of Huddersfield Repository**

Suarez, Jorge Ramiro Perez

We are Cyborgs: Developing a Theoretical Model for Understanding Criminal Behaviour on the Internet

### **Original Citation**

Suarez, Jorge Ramiro Perez (2015) We are Cyborgs: Developing a Theoretical Model for Understanding Criminal Behaviour on the Internet. Doctoral thesis, University of Huddersfield.

This version is available at <http://eprints.hud.ac.uk/id/eprint/28324/>

The University Repository is a digital collection of the research output of the University, available on Open Access. Copyright and Moral Rights for the items on this site are retained by the individual author and/or other copyright owners. Users may access full items free of charge; copies of full text items generally can be reproduced, displayed or performed and given to third parties in any format or medium for personal research or study, educational or not-for-profit purposes without prior permission or charge, provided:

- The authors, title and full bibliographic details is credited in any copy;
- A hyperlink and/or URL is included for the original metadata page; and
- The content is not changed in any way.

For more information, including our policy and submission procedure, please contact the Repository Team at: [E.mailbox@hud.ac.uk](mailto:E.mailbox@hud.ac.uk).

<http://eprints.hud.ac.uk/>

**WE ARE CYBORGS:  
DEVELOPING A THEORETICAL MODEL FOR  
UNDERSTANDING CRIMINAL BEHAVIOUR ON  
THE INTERNET**

JORGE RAMIRO PÉREZ SUÁREZ

A thesis submitted to the University of Huddersfield in  
partial fulfilment of the requirements for the degree of  
Doctor of Philosophy

The University of Huddersfield

December 2015

## **Copyright Statement**

- i. The author of this thesis (including any appendices and/or schedules to this thesis) owns any copyright in it (the “Copyright”) and s/he has given The University of Huddersfield the right to use such Copyright for any administrative, promotional, educational and/or teaching purposes.
- ii. Copies of this thesis, either in full or in extracts, may be made only in accordance with the regulations of the University Library. Details of these regulations may be obtained from the Librarian. This page must form part of any such copies made.
- iii. The ownership of any patents, designs, trademarks and any and all other intellectual property rights except for the Copyright (the “Intellectual Property Rights”) and any reproductions of copyright works, for example graphs and tables (“Reproductions”), which may be described in this thesis, may not be owned by the author and may be owned by third parties. Such Intellectual Property Rights and Reproductions cannot and must not be made available for use without the prior written permission of the owner(s) of the relevant Intellectual Property Rights and/or Reproductions.

## **Dedications**

To my parents:

For their unyielding love, patience and support. My mother kindled my love for law and criminology.

I am ever grateful.

## **Acknowledgments**

Thanks to my supervisors, Bernard Gallagher, Graham Gibbs and Jason Roach that guided, advised me and believed in me for the whole of process.

Thanks to all the staff at the University of Huddersfield, that made this university a home away from home.

Thanks to all the law enforcement agents that dedicated their time to answering my questions, with dedication and kindness.

Thanks to all the people that took time to answer my survey, to the ones who shared it and to the ones who commented on it.

Thanks to Javier Merino, for his invaluable help as a research assistant.

Thanks to Daniel Briggs, for his relevant comments on structure and content.

Thanks to my friends, who cheered me up and didn't let me succumb to despair. Most especially, to Alejandro, Javier, Antonio, Nieves, Lola, Elena, Leanne and Inés.

Thanks to all the people that showed interest in my career and my research in social networks.

Thanks to my students for their interest, their curiosity and their passion in learning criminology.

Thanks to all my colleagues at Universidad Europea de Madrid, for being a great bunch of professionals and fantastic individuals.

Thanks to Maria José Molina, for her consideration in the final moments of my writing process. Also, to Gema Botana and Luis Calandre.

## **Academic Biography**

Jorge Ramiro Pérez Suárez is a qualified solicitor in Spain and a qualified solicitor in Scotland. He has also been awarded with a Masters in Legal Practice in Spain, a MSc in Criminology and Criminal Justice from the University of Edinburgh and was part of the European Young Lawyers Scheme 2016 at the University of Edinburgh.

Jorge has worked as a solicitor in Spain for several years, specialising in criminal law. He has also worked in Scotland as a Procurator Fiscal Depute and at University of Edinburgh as a tutor. Jorge is working full-time for Universidad Europea de Madrid since 2010, where he teaches several criminology modules (both online and campus-based and in English and Spanish) and several online law modules. Jorge also directs and supervises the criminology final project module and directs the student criminology research group at his university. In addition, he supervises the Erasmus programmes for law and criminology and has worked in the forging of a long-lasting relationship with the University of Huddersfield after being invited as a guest academic during 2011.

Jorge is very keen on the use of innovation in education, as his methodologies imply the use of narratives such as short stories, pop culture and poetry in teaching criminology. He has published a book called “Las Crónicas de Enriq” (The Enriq Chronicles) that is both a compilation of short stories and poems for teaching purposes and a short criminology handbook. Jorge is currently co-editing a book on the current state of criminology in Spain.

His areas of interest are cybercrime, sociology of cyberspace, police and policing and innovation in teaching. He is also very active in using social networks for teaching purposes. Jorge is one of the founding members and advisor of the Spanish Association of Criminology Students and has received two awards from the School of Social Sciences at Universidad Europea: one in 2010 for the use of social responsibility in teaching criminology and one in 2011 for his international work with the University of Huddersfield.

**Abstract:**

Technology has supposed a profound paradigm shift in human evolution, following Haraway's cyborg metaphor we have forged a profound psycho-social rapport machines. This connectivity has also brought changes in crime patterns and fostered the development of cybercrime. From a criminological perspective, this work aims to explore the role of Per-Olof Wikströms Situational Action Theory in explaining cybercrime by including Syke and Matza's neutralisation techniques in its formulation. The SAT-RI (SAT- Revised for the Internet) takes into consideration the interaction between cyber-crime propensity (based essentially in moral perceptions), the internet, neutralisation techniques (cognitive scripts used as protection against blame) and self-control.

The theory was tested by using a mixed methods design that includes an online survey (N=709) and case studies (N=20) stemming from interviews with law enforcement agents. Once the data was analysed, it was demonstrated that individuals with low self-control tend to have higher cybercrime propensity and are more prone to justify their acts by using adequate neutralisations. In addition, there are differences in the perceptions of cybercriminals by law enforcement agents depending on whether they are fraudsters, child sex abusers, sex abusers or hackers.

The resulting theory can be useful in terms of prevention, as it can help design programmes that focus on the different stages of the cybercrime process (self-control, propensity or neutralisation). Also, the thesis calls for a more anthropological conception of cyber-criminology called cyborg criminology.

Chapter 1: Introduction	13
Chapter 2: Literature Review	21
2.1. Cybercrime	21
2.1.1. The concept of crime	21
2.1.2. The concept of cybercrime	22
2.1.3. Cybercrime in UK and Spanish legislation	28
2.1.4. Classifications of cybercrime	36
2.1.5. The explanation of cybercrime via criminological theory	38
2.2. Situational Action Theory (SAT)	45
2.3. Situational Action Theory Revised for the Internet (SAT-RI)	56
2.3.1. The internet as an environment	56
2.3.2. Personal propensity for the commission of cybercrimes	58
2.4. Neutralisation Techniques	61
2.4.1. Neutralisation techniques: Sykes and Matza	61
2.4.2. Neutralisation techniques on the Internet	65
2.5. Summary of SAT-RI and Research Questions	70
Chapter 3: Methodology	73
3.1. Aims and Objectives	73
3.2. Research Approach	76
3.2.1. A mixed methods study	76
3.2.2. Epistemology	81
3.2.2. PADS+ as a methodological example of applying SAT	84
3.3. Online Survey on Attitudes Towards Cybercrime	86
3.3.1. Sample	87
3.3.2. Instrument	90
3.3.2.1. Information, consent and demographics	90
3.3.2.2. Self-control scale	92
3.3.2.3. Cybercrime vignettes	94
3.3.3. Procedure	99
3.3.4. Reliability, validity and generalizability	103



3.3.4.1.	Reliability	103
3.3.4.2.	Validity	104
3.3.4.3.	Generalizability	105
3.3.5.	Analysis	106
3.4.	Interviews with Law Enforcement Agents	107
3.4.1.	Sample	107
3.4.2.	Instrument	112
3.4.3.	Procedure	113
3.4.4.	Reliability, validity and generalizability	115
3.4.5.	Analysis	117
3.5.	Ethics	120
3.5.1.	Ethics in an online environment	122
Chapter 4: Findings - Online Survey on Attitudes Towards Cybercrime		125
4.1.	Demographics	125
4.2.	Self-Control Scale	127
4.3.	Vignettes	134
4.3.1.	Morality	137
4.3.2.	Engagement	151
4.3.3.	Neutralisation techniques	163
4.3.4.	Regression	185
4.4.	Discussion	186
4.4.1.	Morality	186
4.4.2.	Engagement	190
4.4.3.	Neutralisations	194
4.5.	Summary	196
Chapter 5: Findings - Interviews with Law Enforcement Agents		200
5.1.	Offender Morality	200
5.1.1.	The professional	200
5.1.2.	Fraudsters without remorse	206
5.1.3.	Hacker morality	210
5.1.4.	Child sex offenders and “internet monsters”	213
5.2.	Offender Neutralisations	220

5.2.1.	Denial of injury	222
5.2.2.	Denial of crime	225
5.2.3.	Appeal to higher loyalties	228
5.2.4.	Fun/just a game	230
5.2.5.	Denial of victim	231
5.2.6.	Robust heterosexual identity	232
5.2.7.	Indifferent attitude	234
5.1.	(Cyber)Police Culture	236
5.1.1.	Mission- action-cynicism-pessimism	238
5.1.2.	Suspicion	240
5.1.3.	Isolation/solidarity	241
5.1.4.	Conservatism	243
5.1.5.	Machismo	247
5.1.6.	Racial prejudice	248
5.1.7.	Pragmatism	249
5.1.8.	Concluding remarks on (cyber) police culture	250
Chapter 6: Integrated Discussion and Validation of SAT-RI Model		253
6.1.	Reformulation of SAT-RI Model	254
6.1.1.	Answering research questions	254
6.1.2.	The SAT-RI “circuit of cybercrime” based upon the online survey	262
6.1.3.	The SAT-RI “circuit of cybercrime” after mixed methods integration	265
6.2.	The Cyborg Construct in the Reformulated Theoretical Model	267
6.2.1.	Cyborg theory redux	267
6.2.2.	Cyborg neutralisation items	272
6.2.2.1.	A capitalistic critique/drive	274
6.2.2.2.	The culture of free	281
6.2.2.3.	The culture of security	285
6.3.	Cybercrime and Gender	292
6.3.1.	Sexuality and pornography on the internet	294
6.3.2.	Sexting, gender and cybervictimisation	299
6.4.	Brief Summary of Current Cybercrime Prevention and Cybercrime Policy	303
6.5.	Limitations	307

Chapter 7: Conclusions	311
7.1. Summary of Findings	311
7.2. Further and Future Research	312
7.3. Implications	314
7.3.1. Prevention programmes based on SAT-RI	314
7.3.2. A new paradigm for approaching cybercrime: "cyborg criminology"	315
References	320
Annex 1: Online Survey	334
Annex 2: Vignettes	345
Annex 3: Vignette Graphs	347
Annex 4: Summary of Cases from Interviews with Law Enforcement Agents	351
Endnotes: Original Excerpts in Spanish	357
Word Count: 87,142	

## List of Figures:

Figure 1. The steps of the perception–choice process in crime causation illustrated. (Wikström, 2010, p. 224) .....	49
Figure 2. The role of the moral filter illustrated (Wikström, 2010, p. 227) .....	51
Figure 3. The roles of motivations, the moral filter and controls in the action processing according to SAT illustrated (Wikström, 2010, p.234) .....	55
Figure 4. Cyberspace (the internet) as a sub-set of the environment .....	57
Figure 5. Cyberspace (the internet) as an environment in itself.....	57
Figure 6. The triangle of cybercrime .....	60
Figure 7. Diagram of the mixed methods design of the SAT-RI study .....	78
Figure 8. Distribution of self-control .....	132
Figure 9. Distribution of Cyberbullying Engagement .....	136
Figure 10. Distribution of Cyberbullying Morality.....	137
Figure 11. Distribution of Revenge Porn morality.....	140
Figure 12. Distribution of Illegal Downloading Morality .....	141
Figure 13. Distribution of Sexting Morality .....	141
Figure 14. Distribution of Wi-Fi Stealing Morality.....	142
Figure 15. Distribution of engagement in Illegal Downloading .....	153
Figure 16. Distribution of engagement in Wi-Fi Stealing .....	153
Figure 17. Distribution of engagement in Revenge Porn.....	155
Figure 18. Means plot for self-control and Sum_Unjustified.....	170
Figure 19. Means plot for Illegal Downloading Engagement and Sum_Unjustified .....	180
Figure 20. Spanish National Police Academy Entrance .....	238
Figure 21. Another detail of Spanish National Police Academy Entrance .....	238
Figure 22. The SAT-RI circuit of cybercrime based upon online survey data.....	262
Figure 23. The complete SAT-RI circuit of cybercrime .....	266
Figure 24. Interview word cloud .....	278

## List of Tables:

Table 1. Situational context and violent action (Wikström & Treiber, 2009, p. 92) .....	54
Table 2. Impulsivity items (Grasmick et al., 1993, p.14) .....	93
Table 3. Advantages and disadvantages of online surveys (Bryman 2012, pp. 676-677).....	100
Table 4. Advantages and disadvantages of online surveys (Hooley, Marriott & Wellens; 2012, pp. 33 and 43 (citing Cantrell & Lupinacci, 2007, 2008; Fleming & Bowden, 2009; Madge et al. 2006)) .....	101
Table 5: List of pseudonyms for law enforcement agents .....	109
Table 6. Descriptive statistics of the Grasmick scale items.....	130
Table 7. Frequency table and graph for the SelfControl_HighLow variable .....	133
Table 8. Correlations between engagement and morality on a case by case scenario .....	135
Table 9. Morality correlations .....	138
Table 10. Morality questions means' comparisons by gender and victimhood .....	143
Table 11. The six elements of self-control mean's comparisons by perceptions of morality...	145
Table 12. Self-control means' comparisons by morality questions .....	148
Table 13. Engagement and morality correlations .....	150
Table 14. Engagement questions correlations.....	152
Table 15. Engagement means' comparisons by gender and victimhood. ....	156
Table 16. The six elements of self-control mean's comparisons by engagement .....	159
Table 17. Self-control means' comparisons by engagement questions.....	160
Table 18. Inconsistencies found when coding neutralisation techniques answers.....	163
Table 19. Frequencies of neutralisation techniques .....	165
Table 20. Self-control means by unjustified (Yes or No) and distribution of unjustified amongst self-control groups .....	167
Table 21. Frequency table for Sum_Unjustified.....	169
Table 22. Comparison of self-control means by all neutralisation techniques and distribution of those who picked neutralisations techniques by Self-Control High_Low (only statistically significant portrayed) .....	171
Table 23. Morality means' comparison by "Unjustified" neutralisation technique .....	173
Table 24. ANOVAs using Sum_Unjustified as factor and morality questions as dependent variables .....	174
Table 25. Comparison of morality means by all neutralisation techniques (only statistically significant portrayed) .....	176
Table 26. Engagement means' comparison by Unjustified neutralisation techniques.....	178
Table 27. ANOVAs using Sum_Unjustified as factor and engagement questions as dependent variables .....	179
Table 28. Comparison of engagement means by all neutralisation techniques (only statistically significant portrayed).....	182
Table 29. Statistically significant neutralisation techniques in relation to self-control, morality and engagement .....	184

## Chapter 1: Introduction

Digital technology has become a central part of human existence. Mobile phones, computers, watches, cars and even kitchen appliances are interlinked via the internet. In parallel, social networking sites (like Facebook, Instagram, YouTube and Twitter) facilitate immediate sharing and editing of pictures and videos, text and voice messages, news and opinions. Those sites also facilitate the discussion of current political and philosophical matters; thus transforming users from mere consumers of information to creators, curators and disseminators of information. In addition, education has been profoundly changed by technology due to the proliferation of distance learning courses. As an example, in higher education, Universidad Europea de Madrid (2015) offers campus-based, distance learning, blended courses and degrees, and there are distance learning universities such as Universitat Oberta de Catalunya (2015), in Spain, or The Open University (2015) in the UK. This digitisation of education has also been fostered by e-books, web-conference platforms and even YouTube tutorials and conferences (see for example Graham Gibbs' (2014, 2015) YouTube channel on research methods). From a different perspective, sexuality can now be expressed by and through the internet due to almost unrestricted access to pornographic content, as well as online dating services and soliciting platforms. Augmented Reality applications, on the other hand, are merging the virtual and real world by adding a "digital texture" to the environment, according to Kipper and Rampolla (2013) "Augmented Reality allows the user to see the real world, with virtual objects superimposed upon or composited with the real world" (Chapter 1, para. 1). In addition, IKEA (2015) catalogues offer an Augmented Reality experience that enable clients to see how the products fit in their homes before buying them. Marvel (2015) also offers Augmented Reality applications that allow readers to access special content in comic-books such as creator commentaries. Another example is Empresa Municipal de Transportes de Madrid (Municipal Transport Company in Madrid) (2015) that has produced an application that

enables iPhones to guide the user to the closest bus stop and gives detailed transport information.

Donna Haraway (1991) talked about the metaphorical “cyborg” - a post-modern entity that addresses the fusion between machine and human being, natural and artificial, biological and mechanical (formulated from a feminist standpoint). All of the changes mentioned above, serve as examples of how the internet has penetrated all facets of human entity and identity in a similar fashion to the cyborg theorisation (i.e. culture, recreation, relationships and sexuality). Subsequently, the internet has reached a mythical status in our society, embedded with quasi-mystical properties. Lives have tightly interconnected matrices, forming a kind of networked society as defined by Manuel Castells (2010) with “information as its raw material” (p. 71), whilst social networking sites have thrived in the culture of “hypernarcissism” (Lipovetsky, 2005). Moreover, the technological medium is also a culture of video-games and online worlds that function as a collective electronic zeitgeist, as argued by Castells (2010) “every cultural expression ... comes together in this digital universe that links up in a giant, non-historical hypertext, past, present and future manifestations of the communicative mind” (p. 403). The computer is thus “a new mirror, the first psychological machine” (Turkle, 2005, p. 279). The mythic status of the internet can also be understood following Baudrillard’s (1988) simulacrum. Baudrillard theorised about the image that started as a reflection of reality, turned into a perversion of reality, then a mask of reality and then became “its own pure simulacrum” (1988). Similarly, Zizek indicates that:

cyberspace merely radicalizes the gap constitutive of the symbolic order: Symbolic reality always-already was “virtual”; that is to say: Every access to (social) reality has to be supported by an implicit phantasmic hypertext (2009, p. 184)

The internet is, thus, conceived as a realm that is consensual, synthetic and may be philosophically real or unreal. It can, ontologically, be a copy of reality, an augmentation of reality or simply another reality in itself. A construction that simulates perverts and then supersedes reality has to contain all single aspects of reality. Crime, inherently understood by some criminologists as part of society, also adapts, changes and evolves; it lives dormant in every human being as if encysted in social structures. Durkheim (2013) recognised how crime was embedded in the fabric of modern societies and served the purpose of unifying citizens by creating threads of solidarity stemming from the shared experience of citizens repulsion towards crime. Durkheim (2013) recognized not only the normalcy of crime, but also its functional purpose as means of advancing society. Criminologists have devoted their experience to trying to map, understand and tackle crime, criminals and the effects of crime in society. A huge corpus of criminological theory explains how crime is a result of psychological phenomena, of social tension and social structure, of psychiatric and neurological complexities, of biological drives and/or a sum of all of these. Criminologists are also concerned with the history and development of crime. Crimes can range from, for example, more conventional violent crime (see for example Agnew, 1992; Wikström & Treiber, 2009) to white-collar (Sutherland 1937, 1983) crime and to crimes against wildlife (Wellsmith, 2012).

Cybercrime is currently, as indicated by the National Police Corp (Cuerpo Nacional de Policía - CNP), one of the major preoccupations of policing agencies in high income countries, being “the third most lucrative crime world-wide” (CNP, 2013b<sup>i</sup>). However, data from Ministerio del Interior (Ministry of Interior) (2013) showed that cybercriminality in Spain in 2013 amounted to only 2% of registered criminal acts (p. 7). Specifically, from the cybercrime data registered in 2013, 62.8 % of crimes were frauds, 21.4 % threats and 4.6 % “crimes against honour” (p. 6). Cybercrime does not, therefore, seem to be excessive in terms of quantity, but law



enforcement agents recognise its seriousness. Furthermore, in 2013 the National Cybersecurity Strategy from the Spanish Government was published, and it indicated that “cybersecurity is a necessity of our society and economic model” (Gobierno de España, 2013, p. 10<sup>ii</sup>).

Cybercrime is an ever-changing phenomenon that develops as fast as digital technology does. According to Europol’s Internet Organised Crime Threat Assessment (2015):

It is a common axiom that technology, and cybercrime with it, develops so fast that law enforcement cannot keep up. Whilst this may be true in some respects, the vast majority of cybercrimes consist of using vulnerabilities that were well known for quite a while. It is the lack of digital hygiene of citizens and businesses (p. 8)

Europol (2015) also indicates that:

Cybercrime is becoming more aggressive and confrontational. The evolution of cybercrime reported in this document shows that there is a shift from hidden, stealthy interventions by highly competent hackers towards direct, confrontational contact between the criminal and the victim, where the victim is put under considerable pressure to comply with the perpetrator’s demands (p. 62)

As an example of current cybercrime trends, agencies like the Children Exploitation and Online Protection Centre (CEOP) in the UK, refer to the proliferation of self-generated indecent images of children (CEOP, 2013b, p.11-12; Europol, 2015, p. 8) that stem from practices such as sexting<sup>1</sup> and can generate cyber-victimisation of children. In addition, Europol (2015) explains current cyber-threats such as the creation of malware like “CryptoLocker” (p. 18), the

---

<sup>1</sup> The practice of taking naked or pornographic pictures and/or videos of oneself and sending it to others via instant messaging applications, SMS, social networking sites or similar applications and sites

use of the Darknet<sup>2</sup> (p. 29) or massive data breaches (p. 40). The Internet Complaint Centre (IC3) from the FBI indicates that “over the last five years, the IC3 received an average of nearly 300,000 complaints per year” (2014, p. 5) and that the total losses reported in 2014 from the complaints that had reported economic loss reached \$800,492,073 (p. 8). The most frequently reported cybercrimes, according to the IC3 (2014), were different types of frauds and scams (including romantic scams and extortion) (pp. 10-14). The IC3 (2014) also indicated that current trends in cybercrime tend to be related to social networking sites (p. 15), schemes related to virtual currency, like Bitcoin (pp. 15-16), and a new type of scam called “business e-mail compromise” that “is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses which regularly perform wire transfer payments” (p. 16). Finally, Europol (2015) warns that “the rise of the Internet of Things (IoT) or the Internet of Everything (IoE) is seen as a major challenge for law enforcement together with Big Data and the Cloud.” (p. 54). The Internet of things (or the internet of everything connects objects between themselves, the internet and software (Servera, 2015).

The the complexity of how cybercrime comes about and its causes are studied in this work. In trying to understand this phenomenon from a new point of view, a revision of criminological theory is explored. Per-Olof Wikström’s Situational Action Theory (SAT) (Wikström, 2006, 2010; Wikström & Treiber, 2007, 2009) is the theoretical core of this work. The reason for choosing SAT is due to its understanding of crime as an interaction between any given environment with a certain set of moral rules (that can or cannot be conducive to crime) and an individual with a certain set of moral rules (that can or cannot be conducive to crime). The theory is used to understand the effects that coming in contact with the internet has in individuals. The SAT also takes into consideration the role of self-control. The environment

---

<sup>2</sup> The non-indexed internet (as opposed to the Surface Web) that cannot be accessed through conventional browsers and guarantees a much higher degree of anonymity.

considered in this study is the internet, which is seen, as conducive to crime or criminogenic in itself because of its particular architecture and characteristics (Miró Llinares, 2011; Newman & Clarke, 2004; Yar, 2005). However, recent literature on cybercrime also seems to emphasise the role of neutralisation techniques in the commission of cybercrimes (Higgins, Wolfe, & Marcum, 2011; Hinduja, 2007; Ingram & Hinduja, 2008; Moore, 2011; Moore & McMullan, 2009, Turgeman-Goldschmidt, 2011). These techniques, following Sykes and Matza (1957) formulation, refer to psychic and social scripts used by offenders to justify their actions and protect themselves from blame, therefore enabling them to commit any given crime. The theoretical development proposed in this work is referred to as SAT-RI (Situation Action Theory Revised for the Internet). The theory measures the propensity for the commission of cybercrime in certain individuals once they come into contact with the internet, and have an adequate catalogue of neutralisations at their disposal.

This thesis is divided in seven chapters:

Chapter 2 addresses all the above mentioned theoretical issues. It discusses the concept of cybercrime and the way cybercrime is addressed in the literature and in legal instruments. At the same time, it explains the SAT key elements as well as the SAT-RI key elements.

Chapter 3 addresses the methodological design of the study; discusses the instruments and the different issues that arose during the data collection process. In this case, the study uses a mixed methods convergent design (Creswell, 2015, pp. 35-36) where the qualitative and quantitative strands of data have similar or equal weight in the study, and are integrated in a penultimate chapter. The methods that were used in this study comprise an online

questionnaire survey and interviews with law enforcement about cybercrime cases they investigated. This chapter also discusses epistemological issues that arise from the mixed methods design.

Chapter 4 presents the data obtained from the online questionnaire survey (quantitative data) and discusses the relationships between the different variables (in this study: self-control, cybercrime propensity comprised of engagement and perception of morality, and the use of neutralisation techniques) by using statistical tests. It sheds light on how cybercrime is perceived by individuals in terms of morality and whether or not individuals might engage in certain cybercrimes. In addition, it indicates the neutralisation techniques that have been chosen by individuals in order to justify their actions and how they affect their cybercrime propensity. The chapter also compares the variables with the sample's measure of self-control obtained from the survey.

Chapter 5 presents the data obtained from interviews with law enforcement agents (qualitative data) in the form of case studies (data obtained from the interviews was broken down into a sample of several cybercrime cases, as explained by law enforcement agents and reflecting the heterogeneity of cybercrime). These cases represent different types of cybercrime investigated by the agents. Given that particular cultural and ideological issues might stem from the data, as they represent institutions of social control exerting power over criminals and society, a discourse analysis was also performed.

Chapter 6 integrates the qualitative and quantitative strands of data, and explicates the final design of the SAT-RI theory. It takes into consideration broader social and cultural issues that

emerged during the quantitative and qualitative analysis, and binds them with the adjusted theoretical model. Finally, it addresses (in a brief manner) issues relating to the prevention of cybercrime.

Finally, Chapter 7 serves as a conclusion of the chapters mentioned above: focusing on future research and the implications of the study.

Overall, this work develops cybercrime theory by trying to understand the psychic rapport forged between individuals and the internet (propensity, neutralisation and self-control when applied to the internet), as well as the perceptions of individuals of internet crime. In addition, it also tries to understand how law enforcement agents investigate cybercrime and how they understand cybercrime and cybercriminals. This exploration of how cybercrime comes about can have repercussions in the prevention of cybercrime, once the theoretical model is tested.

## **Chapter 2: Literature Review**

### **2.1. Cybercrime**

#### **2.1.1. The concept of crime**

Durkheim (2013) discussed the nature of crime in his explanation of the organic society. Such a society<sup>3</sup> is based on the division of labour, its members are interconnected, as if they were organs in a body. Crimes, according to Durkheim (2013) were acts that generate a punishment and “universally they strike the moral consciousness of nations” (Book I, Chapter II, epigraph I, para. 2). The characteristics of every single crime are that they create an intense feeling of repulsion in “normal individuals” as well as offending the collective consciousness of society (Durkheim, 2013, Original annotated table of contents, Book I, Chapter II, epigraph I, para. 2). In summary, according to Durkheim (2013) crimes were understood as an inherent element of society. Crimes are necessary to foster solidarity between individuals (as it generates general repulsion amongst all members of society and elicits a collective response from the system). Crime and punishment are inextricably linked in Durkheim’s (2013) elaboration of the organic society as two necessary facets of the expression of the collectivity.

Gottfredson and Hirschi (1990) defined crime as “acts of force or fraud undertaken in pursuit of self-interest” (p. 15). The authors also signaled the difference between crime and deviant behaviour (pp. 8-14) by indicating that crime generated a formal response from the state, whereas deviant behaviour generated informal group reactions. Crime is, therefore, exclusively castigated by the administrative apparatus, whereas deviant behavior is generated and castigated by social pressure. In other words, according to Goode (2006) deviance is

---

<sup>3</sup> Durkheim (2013) was referring to the society of the late 19th century.

“nonnormative behavior that attracts condemnation” (p. 553). Several authors (see for example, Goode, 2006; Miller, Wright, & Dannels, 2001; Sumner, 1994) discuss whether or not sociology of deviance is “dead” as an academic subject, being one of the reasons for its demise that sociology of deviance has been absorbed by other disciplines such as criminology. Notwithstanding that academic discussion, in the definition of cybercrime presented in this chapter, and used throughout the whole of this study cybercrime is understood as both illegal behaviour and deviant behaviour.

Cornish and Clarke (1986), offered a vision of criminal behaviour based on a rational (albeit limited) decision-making process. This “Rational Choice Theory” (RCT) approach to crime understood crime as the result of a rational process (performed by the criminal) that weighted the means, ends and consequences of crime (even if constrained by situational elements like time and space) and acted accordingly. Also, this approach (Cornish & Clarke, 1986, 1987) considered that different types of crimes required a different decision making processes (for example theft of cash and illegal substance abuse). Another characteristic of the RCT model is that it is not entirely a theoretical construction, but applicable in policy making for the prevention of crime.

### **2.1.2. The concept of cybercrime**

One of the main problems of cybercrime is its heterogeneity; an ever-changing and malleable phenomenon that hindered a proper identification of its key characteristics (see Europol, 2015, for examples on the current evolution of cybercrime). Moreover, a widely accepted definition of cybercrime does not exist in current literature or legal texts (Wall, 2007, 2008a, 2008b).

According to David Wall (2007), cybercrime “is fairly meaningless, because it tends to be used metaphorically and emotively rather than scientifically or legally, usually to signify the occurrence of harmful behaviour that is somehow connected to the misuse of a computer system” (p. 10). Wall (2007, 2008a, 2008b) argued that the term has been widely used by the media with a certain science-fiction inspiration and aspiration.

Others share this notion contending that cybercrime is the use of computer technology to engage in unlawful activity (Brenner, 2007, pp. 382-384, 2010, p. 10). As Brenner (2010) stated “cyberspace becomes the tool criminals use to commit old crimes in new ways” (p. 10). Cybercrime has been presented as a rather vague concept by authors and by different law enforcement actors.

Yar (2005) encountered the same problems when defining cybercrime. As he has stated “A primary problem for the analysis of cybercrime is the absence of a consistent current definition, even amongst those law enforcement agencies charged with tackling it” (p. 409). He also referred to Thomas and Loader’s (2000) definition “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks” (p. 3, cited in Yar, 2005, p. 409). The problems Yar (2005) tried to convey is the absence of uniform definitions of cybercrime (pp. 409-410). Wall (2007), acknowledged the existence of three generations of cybercrimes and of three criminologies of cybercrime. The three generations of cybercrime refer to: the first generation to cybercrimes that merely assisted traditional offending via offender’s use of computers (pp. 44-45); the second one to cybercrimes that spanned through networks (pp. 45-47); and the third to cybercrimes that have been wholly mediated by technology (p. 47-49). In addition, the three criminologies of cybercrime, according to Wall (2007) are: computer integrity crimes, for



example hacking (pp. 52-60), computer-assisted crimes like different types of cyberfrauds, (pp. 69-102, for a detailed explanation of identity crime; see also Wall, 2013); and finally content crimes (pp. 103-129), for instance child pornography crimes.

Jewkes and Sharp (2003) talked about the internet providing “a locus for creative authorship of the self” (p. 3). Important questions were posed by the authors regarding the physical nature of the internet, considering whether the internet is or is not a real place. A mythical conception of the internet seemed to be present as a liquid borderless environment that is somehow real (see Baudrillard, 1988 for a discussion on simulacra) , or at least, echoes the reality people live in : the cyberspace According to Lessig (2006) “[cyberspace] evokes, or calls to life, ways of interacting that were not possible before” (p. 83) and he then distinguished between the internet (a medium of communication) and cyberspace (as some sort of “second life” with a community aspect). The term cyberspace was defined by Michael Benedikt (2000), using metaphorical imagery:

Cyberspace: The realm of pure information, filling like a lake, siphoning the jangle of messages, transfiguring the physical world, decontaminating the natural and urban landscape, redeeming them ... from all the inefficiencies, pollution (chemical and informational) and corruptions attendant to the process of moving information attached to things - from paper to brains- across, over and under the vast bumpy surface of the earth rather than letting it fly free on the soft hail of electrons that is cyberspace ( p. 30)

However, in the next paragraph Benedikt (2000) argues that “cyberspace as just described does not exist” (p. 30). He subscribed to Karl Popper’s ideas as to the existence of three worlds (Benedikt, 2000, p. 1). World 3 is the one that related to the existence of “objective, real and public structures, which are the not-necessarily intentional products of the mind of living creatures, interacting with each other and with the natural world World 1” (2000, p. 31), the

interesting thing about this so-called World 3 is that many of the structures existing there were purely abstract, made of information or patterns. Benedikt (2000) used the idea of *World 3* to explain the existence and characteristics of cyberspace by mentioning four key threads in the evolution of this world. The first one being the idea of myths (pp. 31-32); the second one the history of technology and the development of different technical means (pp. 33-36); the third one the idea of architecture (pp. 38-40); and the fourth and final one the idea of geometry, time and space (pp. 40-42). Subsequently, communications on the internet do not have to be purely synchronous (Message boards, for example, can contain conversations that have a very long life-span and blogs can be accessible as long as the author desires). In relation to space on the internet it must be borne in mind that dimensions such as distance are not operative because of the almost instantaneous access to terminals or contents world-wide. Lessig (2006) also used the idea of architecture in order to explain how the internet regulates itself. The analysis of the three worlds made by Benedikt (2000) and Lessig's (2006) mention of architecture pointed towards the conception of the internet as an abstract "place" where time, space, form, and substance differ from their manifestations in the real world.

Manuel Castells (2010) referred to "real virtuality" (not a virtual reality) when talking about digitized systems of communication and elaborated on what has been discussed above:

A system in which reality itself (that is, people's material/symbolic existence) is entirely captured, fully immersed in a virtual setting, in the world of make believe, in which appearances are not just on the screen through which experience is communicated, but they become the experience. (p. 404)

Cyberspace, the internet and cybercrime seemed to have captured public imagination due to its ubiquity and the permeation of several aspects of our daily lives. The Internet of Things and the Cloud guarantee constant connectivity between objects and individuals. As Servera (2015)

pointed out “the objective is to connect the objects that surround us with people, and at the same time, to connect the objects between each other<sup>iii</sup>”. In relation to this, Europol (2015) warned about the Internet of Things (IoT) and the Cloud, and the ever-present connectivity they generate, understanding it as one of the major challenges that law enforcement agents would face in the future (p. 54). This apocalyptic internet discourse was criticized by David Wall (2008a, 2008b) as he understood it as emotionally charged and nurtured by science-fiction dystopian misconceptions.

Another fundamental problem to be accounted was the amount of physical objects or devices that can be used for the commission of cybercrimes, or against the devices. A plethora of objects have become intertwined with the internet and with human beings, including mobile phones, TV’s and all sorts of gadgets that have been named “wearables”. As an example, according to its web-page, Fitbit products, such as watches and bracelets monitor pulse, weight and sleep and synchronise and share this information with the internet on a 24/7 basis (Fitbit, 2015). From another point of view, Servera (2015) mentioned the use of wearables for the prevention of crime by using emotion detection and Big Data.

It is through continuous contact with machines that the frontiers between human identity and cybernetics become blurred, thus generating what was theorised by Donna Haraway as cyborgs. As Haraway (1991) argued “By the late twentieth century, our time, a mythic time, we are all chimeras, theorized and fabricated hybrids of machine and organism; in short, we are cyborgs” (p. 150). All our lives and routines have been linked to these instruments, and all these instruments have been linked between themselves through invisible threads of information and data. Crimes can be committed whilst comfortably travelling on the train, whilst watching a movie or in the classroom. Thus crime becomes over-reaching by

transcending time and space. It is the age of convergence and connectivity, thus - and as will be explained in further chapters -cybercrime is becoming part of our daily lives, “the criminologies of everyday life” as according to David Garland (2000, 2001).

Moreso, the idea of cyberspace (the environment) as the key element in cybercrime (at least from the architectural point of view) seemed to be emphasised by the new developments in cloud computing (see for example Anderson, 2008; Europol, 2015; Johnson, 2008; Schofield, 2008). As already mentioned, a paradigm shift has occurred in the past few years in relation to the use of the internet and information systems. Instead of using specific physical storage (the user’s hard-drive, for example), personal content is disseminated through different servers all over the world in different platforms, such as Dropbox or Google Drive and also social networks like Facebook, Instagram and Twitter. These new trends have altered the nature of cyberspace towards a more nodal existence, linking with ideas predicted by Lawrence Lessig (2006), about the regulation of markets by themselves and the ability of the internet to also regulate itself. Cyborg theory might have not have predicted that the fusion between the individual, society and the machine would result in the creation of satellite human identity (the fragmented existence of individuals as cloud data in several social networks, web-pages or data storage services). According to Lessig (2006) “cyberspace too arose from the unplanned displacement of certain architecture of control. The tolled, single-purpose network of telephones was displaced by the untolled and multipurpose network of packet-switched data” (p. 2).

One important phenomenon that the current literature has not been really able to address is the idea of the convergence of systems hinted at in previous paragraphs. Smart phones, tablets, TV’s, computers, eBooks, as examples, are all capable of accessing cyberspace in way

or another, to send and receive information, to create networks and links and to share data between themselves.

Subsequently, the idea of cybercrime has been addressed by law enforcement agencies and governments, given its rapid growth and potential for global harm. The Internet Crime Complaint Centre stated in its Annual Report (IC3, 2013, p. 7): “the Internet Crime Complaint Center (IC3) actively pursued its mission to address crimes committed using the Internet” without giving any definition of the term cybercrime.

### **2.1.3. Cybercrime in UK and Spanish legislation**

The European Convention on Cybercrime (2001)<sup>4</sup> addressed the perils new technologies might bring upon us, in terms of crime as well as the challenges in studying the evidence of these crimes. That is one of the main reasons why European countries such as the United Kingdom and Spain are legislating against cybercrime. In this thesis reference is made only to legislation in English and Welsh, and Spanish legislation, in order to present examples of two different legal systems trying to tackle the problem of cybercrime. The reason for doing this is related to the author’s experience and closeness to the British (the essentially the Scottish) and Spanish legal systems<sup>5</sup>. Having said that, the English legal system differentiates between Common Law offences, those contained in Case Law developed by judges and statutory offences, those written in legal texts. In the Spanish legal system, the Criminal Code<sup>iv</sup> is the main legal text in

---

<sup>4</sup> The Convention was signed by Spain and the United Kingdom in 23/11/2001 (later ratified by Spain in 3/6/2010, and by the UK in 25/5/2011). The Convention’s entry into force in Spain took place in 1/10/2010, and in the UK in 1/9/2011.

<sup>5</sup> It must be taken into account that, whilst the England and Wales system is based on Common Law the Spanish legal system is a codified system.

criminal matters and has been subjected to profound amendments in the past few years (for example in 2010 and 2015). Said reforms seemed to be addressing the problem of cybercrime in Spain because of the requirements of European policy. The “problem” of cybercrime is, thus, understood as a crucial key in the European arena (CNP, 2013a, 2013b, Europol, 2015), however legal instruments fail to offer definitions of cybercrime.

The key question in terms of defining cybercrime should be whether or not a general definition of cybercrime is needed or whether cybercrime should be defined according to its different manifestations. Legislators seemed to be favouring the second course of action. Recent amendments of the Spanish Criminal Code served as an example of this with the inclusion of crimes such as child grooming (*Ley Orgánica 5/2010, de 22 de junio por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre del Código Penal*<sup>6</sup> and then the *Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*<sup>7</sup>, hereinafter Spanish Criminal Code (SCC)). In 2010 article 183 *bis* was placed in Chapter II *bis* relating to “sexual assault and abuse to minors of less than thirteen”, within Title VIII of the legal text named “offences against sexual freedom and indemnity”

He/she **who via the internet, phone or any other means of information technology and communication** contacts a minor of less than thirteen and proposes according an encounter with the finality of committing any of the offences described in articles 178 to 183 and 189, provided that the proposition is accompanied by material acts devised to granting the contact ... (emphasis added<sup>v</sup>)

---

<sup>6</sup> Organic Act 5/2010, 22nd june, by which the Organic Act of the Criminal Code 10/1995, 23rd November, is amended.

<sup>7</sup> Organic Act 1/2015, 30<sup>th</sup> march, by which the Organic Act of the Criminal Code 10/1995, 23rd November, is amended.

Following the amendment in 2015, article 183 *bis* became 183 *ter* and Chapter II *bis* “sexual assault and abuse to minors of less than sixteen”. Article 183 *ter* was, then, divided into two sections (183 *ter*.1 and 183 *ter*.2). Article 183 *ter*. 1, indicated that the minor subjected to the contact (grooming) should be less than sixteen. However, article 183 *ter*.2 was enacted as follows:

He/she who via the internet, phone or any other means of information technology and communication contacts a minor of less than sixteen and performs acts devised to ensnare the minor so that the minor facilitates pornographic material or shows pornographic images where a minor appears or is represented...<sup>vi</sup>

Therefore the crime, “*child grooming*” become an autonomous entity in Spanish law. This offence did not refer to committing sexual abuse or aggression to children -which are penalised in different articles -, but to all the preparatory acts using the internet (or any other telematic means) for doing so. The internet was once again understood as a vital instrument in the commission of criminal offences, and in this case, as necessary grounds for an individual to be indicted. Also, the legislator tried to use a “blank formula” when indicating “via the internet, phone or any other means of information technology and communication”. This clause left the door open for any possible technological developments in the near future similar to the internet or phone.

These changes in the regulations of child grooming were mentioned in the in the Preambles of the aforementioned Amendment Acts of the Spanish Criminal Code (from 2010 and 2015). Preambles indicate the reasons for the creation of any given Act in Spain, and discuss its necessity and pertinence.

Stemming from the Council of Europe Framework Decision 2004/68/JHA of 22 December 2003, on combating the sexual exploitation of children and child pornography<sup>8</sup>, Part XIII of the Preamble of the 2010 Acts indicated the necessity of regulating child pornography and child abuse. Part XIII of the Preamble of the 2010 Amendment Act indicates:

On the other hand, the extent of the use of the internet and the technologies of information and communication with sexual intentions towards minors has evidenced the necessity of criminally punishing the conducts that an adult person develops through said media in order to win the minor's trust and organise encounters to obtain sexual favours.<sup>vii</sup>

But this was not the only example of specific cybercrimes that can be found in the current Spanish Criminal Code since the 2010 reform. Title XIII "offences against patrimony and socioeconomic order", Chapter VI, Section I, contained article 248.2 that stated:

Also will be considered liable for fraud:

- a) Those who with an intention of profit and by using any computer manipulation or similar artifice, manage to obtain a non-consented transfer of any patrimonial active in the prejudice of other
- b) Those who manufacture, introduce, possess or facilitate computer programmes specifically designed to the commission of frauds mentioned in this article
- c) Those that by using credit or debit cards, traveller's cheques, or data contained within any of them carry out operations of any kind in prejudice of the card-holder or any other third party. (2010<sup>viii</sup>)

---

<sup>8</sup> This obligation to regulate child abuse also stems from the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse 2007



Article 197 *bis*<sup>9</sup>, punished unauthorised access to data or computer programmes by breaching security measures in place. This breach has to be performed always against the will of the person entitled to exclude the intruder<sup>ix</sup>. What this article contains is the express criminalisation of hacking in the Spanish legal system. In this case, the amendment was performed to satisfy the indications of the Council of Europe Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. Also, the interception of private electronic communications between devices was criminalised in section 197 *bis*. Finally, section 197 *ter*, criminalised the creation of software or access codes for the commission of hacking offences.

The case of including cybercrime in UK legislation seems to be extremely similar to the one in Spain. The pioneering Computer Misuse Act 1990 introduced a series of statutory offences such as “unauthorised access to computer material” (s.1), “unauthorised access with intent to commit or facilitate commission of further offences” (s.2) and, “unauthorised access with intent to impair, or with recklessness as to impairing, operation of computer”(s.3). This is to say, an act for the creation of hacking offences in the UK.

Also, the offence of child grooming was introduced in UK’s legislation under the Sexual Offences Act 2003, it can be read in section 15:

Meeting a child following sexual grooming etc.

[F1(1)A person aged 18 or over (A) commits an offence if— .

[F2(a)A has met or communicated with another person (B) on at least two occasions and subsequently— .

---

<sup>9</sup> since the 2015 amendment

And then, in the very same section:

(a)the reference to A having met or communicated with B is a reference to A having met B in any part of the world or having communicated with B **by any means** from, to or in any part of the world. (2003, emphasis added)

In this case, unlike section 183 *ter* of Spanish Criminal Code that criminalised the contact of minors via the internet, the idea of cybergrooming children in the UK (in this particular section under 16) was contemplated via a blank clause represented by the addition of “by any means” instead of resorting to the mention of the internet and information and communication technologies (ICTs).

In addition, section 8 of the Sexual Offences Act 2003 criminalised “causing or inciting children under thirteen to engage in sexual activity”. But there is no mention of the means used for said purposes. Under British legislation “*child grooming*” is punished as a statutory offence. However, the legislator did not mention the usage of computers, message forums or any ICT’s in the Act. The cybernetic aspect of the crime is purposely forgotten and not included, but this does not mean the offence does not exist.

According to the Child Exploitation and Online Protection Centre (CEOP, 2012) “child sexual exploitation and abuse takes place in both online and offline environments and that the distinction is in many ways artificial to children and young people in 2012” (p. 6). CEOP (2012) also highlights current trends related to consensual uploads of self-generated indecent imagery (SGII) used for social networks profiles, attachments or public video sent or created for their boyfriends/girlfriends that end up being distributed by the receptors “CEOP has seen a marked increase in the number of reports where young teenagers appear to have taken still

or video indecent imagery of themselves which is then shared online” (p. 6). This creates several vulnerabilities for children and teenagers, as they might be subject to extortion or their pictures disseminated without their consent.

More work can be done, however, to identify the sliding scale of risk and harm that accompanies the variety of ways in which SGII is being produced and distributed, and the extent to which these are driven by the malevolent intentions of a third party in grooming, deceiving and threatening children. (CEOP, 2012, p. 7)

Governments, legislators and agencies have finally understood the necessity of tackling the problems that result from cybercrime. For example, according to Ignacio Cosidó (General Director of the Spanish Police (Cuerpo Nacional de Policía)), the fight against cybercrime was one of the major strategic issues for the police as indicated in the Strategic Plan 2013-2016 (CNP, 2013a, 2013b).

As it has been analysed, cybercrime has been catalogued by various scholars, agencies and international bodies, but all fail to ascribe a proper meaning to the word cybercrime. Only its different manifestations are explained and defined. Maybe there is no necessity for such a definition, they were just referring to an umbrella concept or meta-structure as immensely liquid as to being able to contain a myriad of mutating phenomena that change and adapt as fast as technology does. This might be related to Zygmunt Bauman’s “liquid modernity” and his discourse on time and space: “once the distance passed in a unit of time came to be dependant on technology, on artificial means of transportation, all extant, inherited limits of to the speed of movement could be in principle transgressed” (Bauman, 2000, p.9). Bauman (2000) offers a very blunt description of today’s world when contending that: “the insubstantial, instantaneous time of the software world is also an inconsequential time” (p. 118). Jewkes and Sharp (2003) added to that idea, from another point of view by arguing that

“the internet is the postmodern medium ‘par excellence’; the slate upon which we can write or rewrite our personalities in a perpetual act of self-creation” (p. 2). The idea of machines and technology serving as transcendence for the common boundaries of time and space was criticised by Bauman (2000) who reasoned: “even the most advanced technology, armed with ever more powerful processors has still some way to go to attain genuine ‘Instantaneity’” (p. 119). Miró Llinares (2011) talked about the contraction of time and space in cyberspace (pp. 6-10), arguing that cyberspace is real space, yet a new kind of space where the “coordinates of time and space acquire a different meaning and see their scope and limits redefined” (p. 6).

In light of what has been discussed before, three important shortcomings are present in current definitions of cybercrime and the approaches taken by legislators:

- 1) They do not offer an explanation of what cybercrime really is. The term is devoid of meaning
- 2) They tend to focus excessively on the manifestations of crime (like cyberfraud, hacking or child porn offences)
- 3) They do not seem to include manifestations of cyber-deviant behaviour and focus mostly on illegal behaviour.

A more exhaustive definition of cybercrime was therefore needed, one that addresses all forms and manifestations and will endure liquid time. The following is the proposed definition of cybercrime that will be used in this work:

Any action (or lack thereof), be it considered a crime or a legal wrong in any country or a deviation from normalised patterns of behaviour perpetrated via means of ICT (or against any ICT's), that can have consequences on the internet and/or the real world. Said consequences may result in physical and/or psychological damage, economic and/or property loss; loss of dignity, of reputation, of social and/or political stability, of peace of mind or contravention of human rights.

#### **2.1.4. Classifications of cybercrime**

One of the essential features of cybercrime has been its heterogeneity; sex crime, property crime and verbal abuse, for example, fall under the umbrella of the term. It was important to study the different manifestations of cybercrime that have been identified by scholars presented by scholars and to offer a new classification that takes into account the realities presented in the aforementioned definition.

Authors such as Brenner (2010) have divided cybercrimes in three major categories (pp 39-47): target cybercrimes, tool cybercrimes and computer incidental. According to Brenner in target cybercrimes the computer is "broken into" or "bombarded" from the outside (p.39), in tool cybercrimes the computer is the "implement" (p.42) and in computer incidental, "the computer plays a minor role in the offense" (p.45). Following this categorisation, the majority of cybercrimes fall under the label of "tool cybercrimes" (i.e. child grooming, cyber-harassment and cyber-fraud), whereas a small subset relate to the "target cybercrimes" label (for instance, hacking, denial of service attacks and defacement). As for computer incidental, the role played by the computer is related to the offence but is not fundamental to it (for example, making drugs following instructions downloaded from the internet). As indicated in previous

paragraphs, Wall (2007) mentioned the existence of “computer integrity crimes”, “computer-assisted crimes” and “computer content crimes”. Clough (2010) believes there is something of an international consensus surrounding this classification, as it stems from the one used by the US Department of Justice.

These three categories are interesting from the point of view of the present work, but a more criminological classification could be added, one that takes into consideration the different manifestations of crime (traditional, non-cybernetic crime) in criminological literature as according to their targets. The following is the suggested classification:

***a) Violent cybercrime:***

1. Violence against the person (for instance, cyberbullying and cyberstalking.)
2. Violence against systems (for instance, hacking, denial of service and defacements.)

The latter was equivalent to “target cybercrimes” and “computer integrity crimes”, as the offence would be directed towards the computer. A violent component is understood to exist in this type of crime, as the destruction or corruption of systems is sought. In addition, when talking about violence against the person, one could argue that a similarity exists between “tool cybercrimes” as the computer was the vehicle by which the offence is committed. However, these types of cybercrimes seek the “destruction” of the person (instead of the system) albeit in a metaphorical manner by intending to destroy his/her reputation, dignity or peace of mind. These types of crime could also be considered “computer content crimes” (Wall, 2007) and a species of “identity crime” (Wall, 2013).

**b) Sexual cybercrime:** for example child pornography, some types of stalking, and grooming. Some of these crimes could also have a violent element and might be considered a hybrid between these categories and the first one (for instance, some types of cyberstalking). In this case, even though they should have been considered tool cybercrimes, the goal is purely sexual (to obtain sexual gratification). Also, these types of crime fall under Wall's (2007) conception of "computer content crime".

**c) Property cybercrime** (especially cyberfraud): including spam, identity theft and intellectual property crime. All of these crimes imply an abuse of property or use rights, including fraud, and they also tend to involve economic loss. These types related to Wall's (2007) "computer-assisted crime" but also Wall's (2013) "identity crimes".

**d) Socio-political cybercrime:** Cyber-terrorism or hacktivism<sup>10</sup> would be good examples. These types of crimes aim to disrupt social or political stability.

### **2.1.5. The explanation of cybercrime via criminological theory**

From a general point of view, cybercrimes are essentially opportunistic (Newman & Clarke, 2003). Yar believed that "novel sociointeractional features of the cyberspace environment (primarily the collapse of spatial-temporal barriers, many-to-many connectivity, and the anonymity and plasticity of online identity) make possible new forms and patterns of illicit activity" (2005, p.411). In addition, Newman and Clarke (2003) advocated for the prevention of

---

<sup>10</sup> Hackers pursuing a political agenda, usually trying to achieve a higher democratic order or trying to fight a democratic order that is understood as unfair or corrupt. The Anonymous movement serves as an example

e-commerce fraud by using Situational Crime Prevention, following also Cornish and Clarke (1986, 1987). This approach, from a theoretical standpoint, was based in four different assumptions: the limited rationality of crime; the modification of situations to hinder the commission of crimes; the secondary importance of personal predispositions in understanding crime; and the relation between crime prevention and the motivation of offenders (Newman & Clarke, 2003, p.7). The internet can become an extremely criminogenic setting, according to Newman and Clarke (2003): "the prime ingredient of cyberspace is information, that both defines and constructs situations in which crime occurs" (p.10). Information has been considered to be an extremely "hot product", a product that possesses profound criminogenic qualities following Clarke's CRAVED acronym (information is Concealable, Removable, Available, Valuable, Enjoyable and Disposable) (Newman & Clarke, 2003, p. 68, citing Clarke, 1999). The CRAVED acronym could be crucial when explaining different types of cyber-frauds, yet it does fail to include the peculiarities of, for example, violent cybercrimes and sexual cybercrimes. However, an element of limited rationality and opportunism might be found behind the offender's motivation (Cornish & Clarke, 1986, 1987). In addition, Clough (2010) talks about scale, accessibility, anonymity, portability and transferability, global reach and absence of capable guardians as the "key features of digital technology which facilitate crime and hamper law enforcement" (p. 5). Similarly, according to Europol (2015), the main issues in terms of investigative challenges were "attribution, anonymisation, encryption and jurisdiction" (p. 9). The internet is considered as a criminogenic setting in itself given its particular characteristics. It is complicated to prove (not only in legal terms) who committed any given cybercrime but also where the cybercrime was committed and where it should be tried.



In contrast, David Wall (2008a) stated that:

Intertwined with the innate distrust of internet users is the fairly widespread view that not only does the internet place individuals at risk, but it can also corrupt normally law-abiding individuals who go on a moral holiday when on the internet. The internet certainly broadens internet users' life experience and exposes them to a range of social activity that may be outside the confines of their everyday life (p. 875)

Wall warned against the mainstream and media-constructed discourse on the dangers on the internet. From his point of view, the realities of internet are "the reorganisation of criminal labour online" (2008b, p. 55), and the already discussed three generations of internet crime and three offending patterns (hacking, content crime and computer-assisted crime) (p. 55; see also Wall, 2007). Wall explained that cybercrime was starting to follow certain patterns of specialisation that mirror market structures (for example, outsourcing certain services). In a very similar fashion, Europol (2015) seemed to point to a trend towards collaborative work between certain cybercriminals (p. 64) and the concept of "crime-as-a-service" (p. 64). However, these realities did not seem to contradict the fact that certain intrinsic features of the internet attract the commission of crime.

In relation to Routine Activity Theory, a triptych comprising the "motivated offender", "the absence of capable guardians" and "the suitable target" is used to explain the commission of a crime. Said triptych is obviously dependent on variables of time and space (see Yar, 2005, pp. 415-418 for a discussion on the spatiality and temporality of the internet), and is closely linked to the idea of "hot products" (or suitable targets). Yar used Felson's VIVA (Value, Inertia, Visibility, Accessibility) concept instead of Clarke's (1999) CRAVED notion, to explain the qualities of eventual targets (Yar, 2005, pp.418-422). Targets (whether they operate in economic or leisure realms) on the internet tend to be valuable, they possess a certain amount

of weightlessness (inertia), the internet is a public medium (visibility) and the internet is very easy to access but at the same time easy to get away from, owing to the anonymity it grants (accessibility).

The “absence of capable legal guardians” (as argued by Clough, 2010; Grabosky & Smith, 2001; Yar, 2005, pp. 422-423) facilitates the committing of internet related crime. The concept of absence of legal guardians and lack of deterrent qualities might be understood as facilitators that boost the opportunity for the commission of deviant acts. However, Yar (2005) concludes that:

it would appear that RAT’s concept of capable guardianship is transposable to cyberspace, even if the structural properties of the environment (such as its variable spatial and temporal topology) amplify the limitations upon establishing guardianship already apparent in the terrestrial world .(p. 423)

Grabosky (2001), and Grabosky and Smith (2001), talked about different motivations for the commission of computer crime, namely lust, greed, hatred, political views or revenge. Grabosky and Duffield (2001) mentioned the concept of “ego challenge” (and also echo Robert Agnew’s types of strain as motivators, Agnew, 1992; Agnew, Brezina, Wright, & Cullen, 2002). By contrast, KPMG’s (2007) survey on the profile of an online fraudster indicated, from a theoretical point of view, that fraud is a triangle that comprises motivations, opportunity and rationalization; “financial pressure resulting from a fraudster’s excessive life style” (p.2) being one of the essential motivations for offenders.

On the other hand, theories such as Merton's (1968) could be used as a more specific template for fraud motivations (and even other types of crimes) as they try to specify the strain and frustration that certain individuals face once they fail to reach certain legitimate social goals (these goals are essentially pecuniary). This results in a social state of normlessness where individuals innovate and "adapt through the use of institutionally proscribed but often effective means of attaining at least the simulacrum of success-wealth and power" (Merton, 1968, p.141; see also Agnew, 1992; Agnew et al. 2002). According to Robert Agnew, the individual can face three types of strain: strain produced because of the anticipated failure to achieve positively valued goals; strain produced because of the removal of positive stimuli; and strain produced by actual or anticipated noxious stimuli (Agnew, 1992; Agnew et al., 2002). Agnew's theory, despite having more reach than Merton's, was also incomplete when applied to cybercrime, because as he himself explained, individuals have a catalogue of coping mechanisms that can protect them from suffering such strain, and therefore avoid crime (Agnew, 1992). In a current study about illegal downloading and its relationship with self-control and Strain Theory, Hinduja (2012) concluded that "The results suggest that individuals do not download music illegally because they are experiencing strain" (p. 961). This study by Hinduja (2012) indicates how Strain Theory is not the cause behind the commission of music piracy (illegal downloads).

Finally, Sutherland (1937, 1983) explained that White Collar crime is rooted in a "differential association", meaning that "criminal behaviour is learned in association with those who define such criminal behaviour favorably and in isolation from those who define it unfavorably" (Sutherland, 1983, p.240). Then "if the weight of favorable definitions, exceeds the weight of the unfavorable definitions", the individual will resort to crime (p.240). Sutherland (1983) also pointed out the importance of a state of "social disorganisation" that can be considered as

either anomie, or the “lack of social standards which direct the behavior of members of a society in general or in specific areas of behavior” (p. 255). Sutherland’s theory has been used in criminology as an explanation of white-collar crime and theft (both being economic crimes), indicating that individuals commit these crimes after a process of “tutelage” by other individuals that transmit the values, techniques and motivations behind crime. Authors such as Herrero Herrero (2007) have classified cybercrime as a type of economic crime. In this thesis, however, that is not the case. Although Sutherland’s theory (1937, 1983) seems insufficient to explain cybercrime, the part about “social disorganization” and “lack of social standards” can serve as an explanation of the absence of strong moral rules on the internet. In addition, Sutherland’s differential association theory could help explain certain types of cybercrime that stem from a corporate structure. As indicated earlier, it must be recognised, that understanding cybercrime as a sub-type of economic crime would be an extremely narrow view, as it explains some types of cyberfraud, and yet fails to explain sex-related crimes, “*child grooming*” or cyberbullying.

In relation to “self-control theory” (Gottfredson & Hirschi, 1990), crimes are committed by individuals with low self-control, as they are unable to postpone the satisfaction of desire and pleasure. Crime is, according to these authors, the best way to satisfy an instant necessity as well as being extremely gratifying, thrilling and easy to commit at the very same time. Gottfredson and Hirschi elaborated a static conception of self-control, one that was forged during infancy and remained constant throughout adulthood. Can a lack of self-control explain the commission of cybercrimes? Are cyber-criminals individuals with low self-control who resort to the internet as the easiest way to satisfy their predatory impulses? It is very difficult to refer to self-control (in Gottfredson and Hirschi’s conception) in relation to cyber-criminals, taking into account studies mentioned earlier such as Moore and MacMullan’s (2009) and

Hinduja (2012). Individuals involved in illegal downloading might be law-abiding citizens who are able to neutralise the deviant component of said offences by using different cognitive scripts.

All in all, current criminological theory does not seem to produce a clear explanation of the reasons behind the commission of cybercrimes. It might be able, up to a point, to explain the opportunistic and situational factors inherently linked to the nature of cyberspace (absence of capable guardians, motivated offenders and information as a hot product) but not the aetiology. Sociological explanations of crime also fail to explain cybercrime as social conflict (the individual versus society, frustration). Self-control or differential association could explain facets or manifestations of cybercrime but not the whole of cybercrime. Neutralisation theory, on the hand, has offered better results. Eclectic or multi-factorial explanations of crime are to be taken into consideration by criminologists in order to explain the reasons behind the commission of cybercrimes, but what is proposed in this thesis is the development of one of the most over-reaching current theories into a new paradigm that includes the specificities of cyberspace and cybercriminals, and links endogenous or personal variables with exogenous or environmental variables.

## **2.2. Situational Action Theory (SAT)**

The essential aspect of Situational Action Theory of Crime Causation is that it considers crime to be the result of a process of deliberation, a moral choice (Wikström, 2006; Wikström & Treiber, 2007; Wikström & Treiber, 2009; Wikström, 2010). This theory defers from Newman and Clarke's (1986, 1987) rational approach by emphasising the importance of morality in the decision-making process.

This theory aimed to be considered a general theory of crime, overcoming the problems encountered by major criminological theories (according to Wikström). Namely, a clear definition of what crime is, what is it that moves people to engage in acts of crime, the interaction between environmental factors and personal factors, and the role of social conditions and individual development (Wikström, 2010). It is, therefore, an eclectic theory, one that takes into account social factors (the environment in itself, the rules of said environment and the moral context) and personal factors (the moral make-up of the individual, his/her tendencies and habits, as shall be explained below) and linked them. Sociological theories have been mentioned earlier, for example, "differential association" (Sutherland, 1937, 1983) - explaining how individuals learn criminal motivations and techniques from others. Other theories have also been mentioned, relating to the criminogenic frustration and strain generated by the inequality between societal goals and means to achieve them (Merton, 1968; see also Agnew, 1992; Agnew et al. 2002). Similarly, "self-control" theory (Gottfredson & Hirschi, 1990) has been put forward to explain how any given individual's self-control (his/hers capacity to cope with frustration and need for immediate pleasure) is forged by his/her parents during infancy. These theories describe the interaction between the individual and others or the individual and society. On the other hand, SAT, considers both societal variables and personal variables, understating how their linkage

generated a moral process of deliberation resulting in an eventual act of crime. Wikström (2010) stated:

I submit that mainstream criminological theory generally (not all theories in all respects but all theories at least in some respects) fail to fully address:

(i) what crime is (to clearly define what it is the theory aims to explain),

(ii) what it is that moves people to engage in acts of crime (to present an adequate action theory),

(iii) how personal and environmental factors interact in moving people to engage in acts of crime (to properly integrate key insights from personal and environmental explanatory approaches),

(iv) the role of broader social conditions and individual development (life histories) (to analyse their influence not as causes but as causes of the causes). (pp. 213-214, also Wikström & Treiber, 2009, p. 78)

These points cited above of paramount importance in order to understand SAT as one of the most comprehensive criminological theories of current times. Its eclecticism was manifested when Wikström explained how theories such as Gottfredson and Hirschi's focused on individual differences whereas other theories focused on the environment "Nevertheless, such accounts rarely provide any elaborate attempt to integrate individual and environmental factors in crime causation" (Wikström, 2010, p.215). Another relevant criticism made by Wikström (2010) is that "criminological theories often ignore the role of agency" (p. 225). The following paragraph sums up the preceding point and presents in a very concise manner the key elements of SAT:

Crimes are moral actions so what we need to explain acts of crime is a theory of moral action; an action theory that explains why and how people are moved to carry out acts in

compliance with or in breach of rules of conduct. Such a theory helps us focus our attention on what kinds of personal and environmental factors may be relevant in the explanation of acts of crime. (Wikström, 2010, p. 214)

When explaining the SAT, Wikström (2006) emphasised the relationship between the individual's actions, motivations, and moral values and the setting: "the action a particular individual takes is always a result of the features of the settings in which he takes part and his processing and evaluation of the environmental input" (p.93). Thus, Wikström indicates the creation of a moral context that leads to the formulation of a moral choice. The environment is defined as "all that is external to the individual and that with which he comes into contact" (p. 86). He expanded the definition by stating that:

The individual's environment can be conceptualised as his activity field. An activity field may be defined as the configuration of the settings in which the individual takes part during a particular period of time (e.g., his daily activity field or his annual activity field). A setting might be defined as the social and physical environment (objects, persons and events) that the individual, at a particular moment in time, can access with his senses (e.g., what he can see, hear and feel) this also includes everything he can see, hear and feel through the exposure of various media (e.g., television, radio, telephone, computers, newspapers, books, etc.) present in the setting. (p.86)

The relevant question arising from this explanation should be: is the internet a proper setting? In order to develop SAT to explain cybercrime, and drawing on the conceptualisations advanced in previous paragraphs (relating to the specific geo-spatial characteristics of the internet that refer to the contraction of time and space as already indicated by Miró Llinares (2011, pp.6-10), it shall be indicated that it is. When the individual is connected to the internet



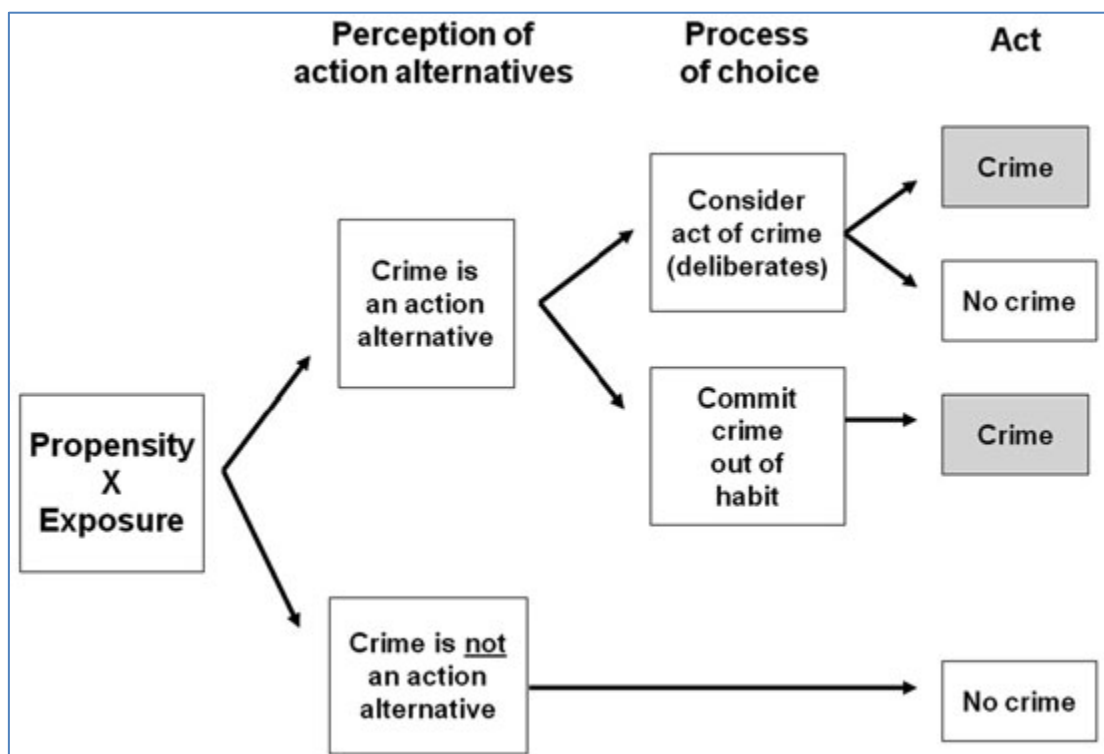
from any given environment (his/her home, for example), his/hers decision whether to commit an act of moral rule-breaking is not entirely linked (as it is hypothesized in this work) to the moral characteristics of the physical environment but to the moral characteristics of the non-physical environment (the internet). That internet environment is independent from the physical environment and its moral rules and/or deterrent qualities. However, one could argue that both environments (and their qualities) might be connected in a certain way (if the internet is conceived as a simulacrum of reality or as a virtual reality, see Baudrillard, 1988; Castells, 2010). Also (according to the hypotheses presented in this work), the propensity of the eventual offender varies depending upon whether he/she is considering moral rule-breaking in the physical environment or in the real life environment. This is closely linked to the idea of neutralisation techniques developed in further paragraphs. The internet, therefore, is considered an environment in itself, unrelated to where it is accessed from, but related to whom it is accessed by.

Subsequently, Wikström (2010) explained the situational model by indicating the existence of four key elements: person, setting, situation and action. Therefore moral actions can be understood as an outcome of situational processes:

the concept of crime propensity refers to the personal factors that affect a person's likelihood to perceiving an act of crime as an action alternative and carrying it out, in response to a particular setting ... This general reasoning **is also applicable to analyses of specific kinds of crime, in which case we would talk about [type of crime] propensity,** for example shoplifting propensity or partner violence propensity. (p. 220, emphasis added)

This is one of the reasons why SAT can be used for explaining cybercrime, as there are certain aspects of it (especially the legally and morally liquid setting) that require certain types of personality traits. For Wikström (2010), there is an intersection between the individual's propensity to engage in acts of crime and in his/her exposure to criminogenic settings (Wikström, 2010). Therefore, Propensity x Exposure = Crime (Wikström, 2006; Wikström & Treiber, 2007; Wikström & Treiber, 2009; Wikström, 2010). This deliberation process leading to crime is explained in Figure 1.

**Figure 1. The steps of the perception–choice process in crime causation illustrated. (Wikström, 2010, p. 224)**

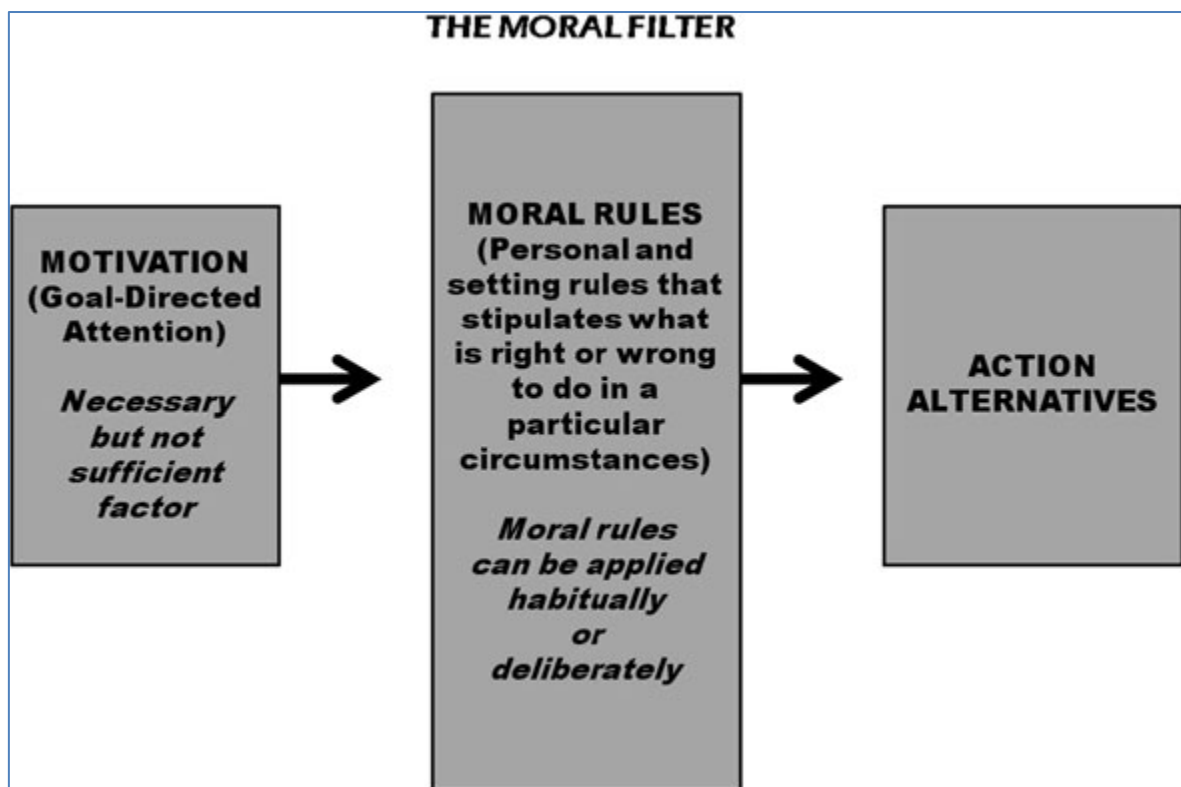


In order to understand Figure 1, it is important to mention another key concept in SAT: the role of motivation or goal-direction attention (Wikström, 2010, p.226). It is important to note that “It is necessary because to act people first have to be motivated to do so, but it is not

sufficient because no particular motivation (goal-directed attention) in itself always causes people to breach a moral rule (defined in law)”(Wikström, 2010, p. 226; see also Wikström & Treiber, 2009 pp. 80-81). Individuals might wish to commit a crime (for example to hit someone or to steal expensive clothing from a shop) yet this desire alone (according to the SAT framework) will not result in an actual law-breaking act. Motivation is, therefore, a situational concept that stems from the relationship forged between the individual and the environment, and which originates from temptation or provocation (for definitions and further discussion on the matter, see Wikström, 2010, p. 226 and Wikström & Treiber 2009, pp. 85-86). So, what exactly will make a motivated individual abstain from an act of shop-lifting? Or in other words, what will make the individual perceive his/her motivation to steal as an action alternative? The answer is the *moral filter*, defined as “the moral rule-induced selective perception of action alternatives) circumscribes what actions are perceived as appropriate in response to a particular motivation” (Wikström, 2010, p. 227). Also in relation to motivations, “the ability to exercise self-control (controls that are internal in origin) and (ii) deterrence (controls that are external in origin) are the core potential inhibitors of a particular motivation” (Wikström & Treiber, 2007, p.249). Once again, the idea of internal and external factors correlating has been posited as the very crux of SAT.

Going back to the moral filter, it can be argued that it can be applied in a semi-automated way (out of moral habit) or can be used as a pattern for moral deliberation. The role of the moral filter, explained in the previous paragraph, is depicted in Figure 2.

Figure 2. The role of the moral filter illustrated (Wikström, 2010, p. 227)



Finally, the last key concept in relation to SAT is the role of self-control. As self-control “may only come into play, (become causally relevant) when a person is motivated and sees an action that would breach a rule of conduct as an alternative to satisfy the motivation” (Wikström, 2010, p.229). Self-control has been mentioned as the essential element in Gottfredson and Hirschi’s General Theory of Crime (1990) and defined as “the tendency to avoid acts whose long-term costs exceed their momentary advantages” (Gottfredson & Hirschi, 1990, p.3 , cited in Wikström, 2010, p.231) and has always been regarded a “stable individual trait” (Gottfredson & Hirschi, 1990, cited in Wikström, 2010, p. 231). However, there is within SAT, a radical re-conceptualisation of self-control, where it is seen as:

[A]situational process (and not, for example, a person’s impulsivity or police presence in a setting), defined as the cognitive process by which people manage conflicting rule-guidance when deliberating whether or not to act upon a particular motivation that

involves a breach of a rule of conduct (Wikström, 2010, p. 232 also explained in Wikström & Treiber, 2009, pp.79-80 and Wikström & Treiber, 2007, p.243).

This conception of self-control was very novel as it differed from accepting self-control as a static internal trait. SAT developed self-control into a dynamic situational concept that depended not only on individual characteristics, but also on environmental characteristics relating to the setting. As Wikström and Treiber (2007) explained:

We argue that self-control is best analysed as a situational concept rather than an individual trait. We submit that an individual's ability to exercise self-control is an outcome of the interaction between his/her executive capabilities (an individual trait) and the settings in which he/she takes part (his/her environment). (p.238)

This is the reason why "self-control comes into play in the process of choice only when the temptations and provocations an individual faces in a particular setting conflict with his/her moral rules" (Wikström & Treiber, 2007, p.243). However, in relation to the relative importance of self-control, it must be noted that "the primary reason for individuals' law abidance is strong moral beliefs (and moral habits) that correspond to the moral rules of the law, rather than their ability to exercise self-control" (Wikström & Treiber, 2007, p. 250). To develop what has been said, according to the results of a study by Wikström and Svensson (2010), self-control plays decisive role only when individuals have weak morality. When individuals are able to contemplate the possibilities of committing crimes, in their own words "both personal morality and the ability to exercise self-control are important factors for a person's crime involvement, (ii) personal morality is the more fundamental of the two since the role of a person's ability to exercise self-control in predicting crime involvement is conditional on his or her personal morality" (Wikström & Svensson, 2010, p.405).

This connection between personal morality and self-control is one of the major reasons why SAT becomes a crucial instrument when trying to understand the reason why people engage in acts of cybercrime, especially why law-abiding citizens might consider cybercrime as an action alternative. This is also the reason why SAT is being presented as a template for the explanation of cybercrime by adding new variables to the theory.

It is, therefore also necessary to talk about the deterrent qualities of the setting. As “if there is an *effective monitoring* of and *effective sanctioning* of moral rule-breaking, the setting has strong *deterrent qualities*” (Wikström, 2006, p.101; see also Wikström & Treiber, 2007). Wikström also contended that “casually relevant environmental factors that affect the criminogenic exposure a setting provides are (iii)the moral rules of the setting, (iv) their level of enforcement (through the process of deterrence)” (Wikström, 2010, p.221). This can be connected to Yar’s (2005) work on Routine Activity for the Internet. The apparent lack of capable guardians (with deterrent capabilities) has already been discussed in previous paragraphs. Yar (2005) concluded that they exist, even if the internet has intrinsic limitations in terms of guardianship.

In Table 1, the relation between Propensity and Exposure to a moral context is explained in relation to violent crime. If the context is conducive to violence and the individual’s propensity is also conducive to violence, violence is likely to happen. However, if the individual’s propensity is not conducive to violence but the context is, violence will depend on the actor’s ability to exercise self-control. This is a relevant in relation to the internet, as it is important proving that cyberspace is conducive to crime (not only violent crime, but any kind). Should

that be proved, the commission of cybercrimes would rely solely on the individual's capacity to exercise self-control (as a situational concept, not as a static one). The fact of considering whether the internet is conducive to crime lies once again on the very specific characteristics of the internet hindering the capacity for self-control (especially anonymity). On the internet, the idea of self-control might be profoundly interwoven with the ideas of neutralisation and rationalisation of conducts.

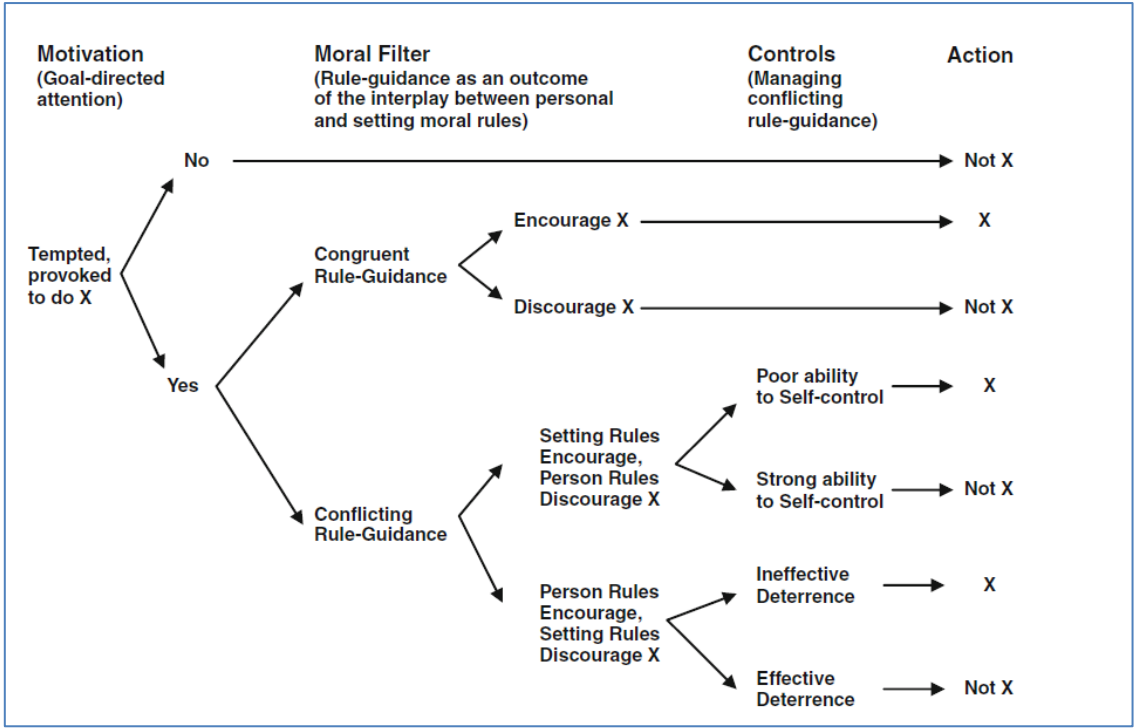
**Table 1. Situational context and violent action (Wikström & Treiber, 2009, p. 92)**

Situational Context		
Propensity	Exposure to Moral Context	
	Conducive to violence	Not conducive to violence
Conducive to violence	Violence is likely	Violence will depend on the level of deterrence
Not conducive to violence	Violence will depend on the actor's ability to exercise self-control	Violence is unlikely

In order to sum up the intricacies of the theory being discussed in this chapter, Figure 3 illustrates the SAT process by explaining the role of motivators, the moral filter and controls, as a flow chart. If the individual faces motivation (he is tempted to do something), and there exists a moral filter that implies congruent rule-guidance encouraging the commission of an action, then the action will be committed. However, if this moral filter is congruent in terms of rule-guidance and discourages the commission of a crime, the action will not be committed. In contrast, if the moral filter implies conflicting rule-guidance, then the rules of the setting and/or the rules of the person will be the ones dictating the commission of an action, depending on the capacity of the person to exercise self-control or the deterrent capabilities of the setting. Wikström, Oberwittler, Treiber, and Hardie (2013) conducted a longitudinal study

of juvenile urban crime in Peterborough known as the Peterborough Adolescent and Young Adult Development Study (hereinafter PADS+). Wikström et al. (2013) measured certain personal and environmental variables. through time, using the SAT theoretical framework. They measured self-control and crime propensity, activity patterns and the perception-choice process. The instruments used by Wikström et al. (2013) are discussed in more depth in Chapter 3 (Methodology).

**Figure 3. The roles of motivations, the moral filter and controls in the action processing according to SAT illustrated (Wikström, 2010, p.234)**





## **2.3. Situational Action Theory Revised for the Internet (SAT-RI)**

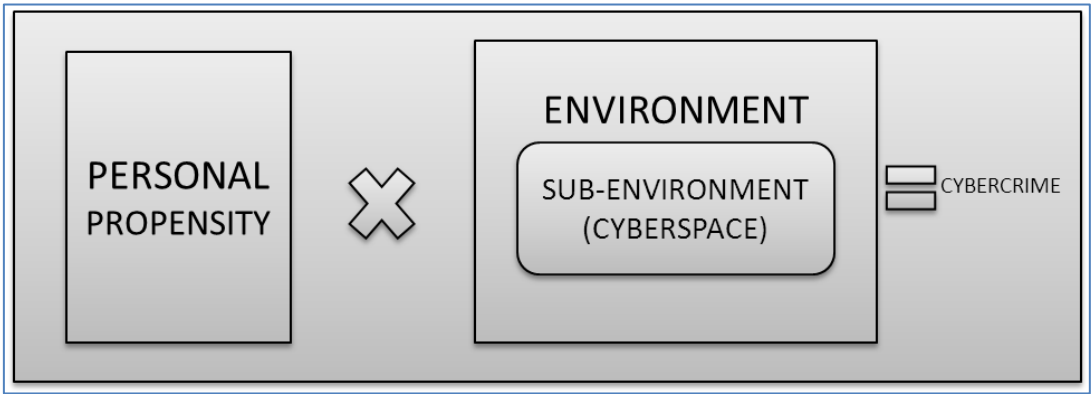
As indicated in previous paragraphs, SAT is a general theory that aims to overcome the problems presented by current and past criminological theorisations and it offers an over-reaching explanation of all types of crime (including causes of crime and causes of the causes) (for an in depth explanation see Wikström, 2010, pp. 213-216, also Wikström et al., 2013). One might argue that such a complex theory suffices to explain the phenomena of cybercrimes. However, the formula  $\text{Propensity} \times \text{Exposure} = \text{criminal action}$ , might generate some troubling issues when addressed in this work in relation to the internet.

### **2.3.1. The internet as an environment**

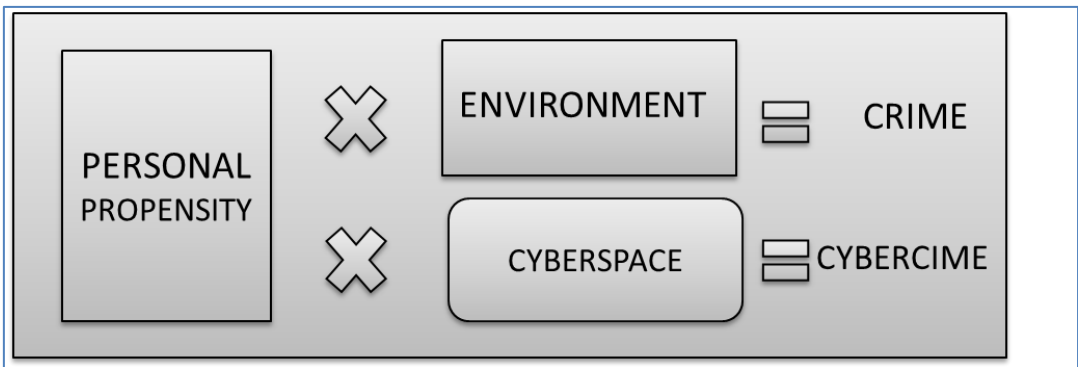
It should be borne in mind that the exposure variable refers to the feedback established between the individual, and an environment that has its own set of moral rules and deterrent qualities. However, the internet exists as a juxtaposed and simultaneous reality; the internet is in itself an environment (virtual reality) within another environment (the physical world). Any kind of crime committed by using any information and communications technology (ICT), against any person or ICT (see definition of cybercrime provided in this work) is not entirely caused by the context the ICT is accessed from. Such a crime is also caused by the context of the internet and the personal moral variables of the offender. In other words, when considering the “exposure” variable, a specific environment is mentioned (internet) that does not need to relate to the physical environment the offender was immersed in. Figure 4 depicts the internet as being immersed in another environment (i.e. a community, a country or a town) and thus, the internet, sharing the moral norms of the offline environment. In Figure 4, cybercrime is caused because of the interaction between personal propensity and both environments

(online and offline). On the other hand, Figure 5 depicts the internet and the offline environment as autonomous environments (the individual can come into contact with either the online or the offline environment) and the crimes that result will be different. When the individual comes into contact with the online environment, and his/her personal propensity is conducive to crime, he/she might commit a cybercrime. This thesis also explores whether there is a specific personal propensity for the commission of cybercrimes (cybercrime propensity).

**Figure 4. Cyberspace (the internet) as a sub-set of the environment**



**Figure 5. Cyberspace (the internet) as an environment in itself**



In this thesis, the formulation presented in Figure 5 is the one to be considered for the update of SAT in order to explain cybercrime. In SAT-RI (Situational Action Theory Revised for the Internet), the only environment that is considered is the internet - as an autonomous moral context, unrelated to the offline moral context. The internet is viewed as having its own set of moral values and normative by which it regulates itself (see Lessig, 2006 for a detailed explanation of how the internet regulates itself). Therefore, when talking about SAT-RI, this author will consider only interactions that occur when individuals come into contact with the internet.

### **2.3.2. Personal propensity for the commission of cybercrimes**

According to current literature, cybercriminals might justify the commission of their offences via cognitive scripts called neutralisation techniques, which Sykes and Matza (1957) explain serve as a “protection from the self-blame and the blame of other after the act” (p. 666). These cognitive scripts stem from the idea that the offender does not belong to a particular subculture of wrongdoers: “if there existed in fact a delinquent subculture such that the delinquent viewed his illegal behavior as morally correct, we could reasonably suppose that he would exhibit no feelings of guilt or shame at detection or confinement” (Sykes & Matza, p. 664).

The idea of neutralisation techniques will be developed in further paragraphs of this chapter and they will be used to explain why “law abiding” citizens can resort to law-breaking practices (for example, illegal downloading). In addition, some types of crimes might require a specific set of personality traits (for example, hacking or cyberfrauds) as already pointed out by Grabosky (2001), and Grabosky and Smith (2001). According to the authors (Grabosky, 2001;

Grabosky & Smith, 2001; see also KPMG, 2007, 2011) in relation to frauds, those personality traits can be: lust, hatred, and ego challenge. However, it is not entirely clear how those traits can be extrapolated to a general population of cybercriminals. One could argue that the personal propensity for the commission of cyberfrauds or cyberbullying is the same as the one for the commission of “traditional” forms of fraud and/or bullying, with a mere addition of an opportunistic element (see Cornish & Clarke, 1986, 1987; Miró Llinares, 2011; Newman & Clarke, 2003; Yar, 2005).

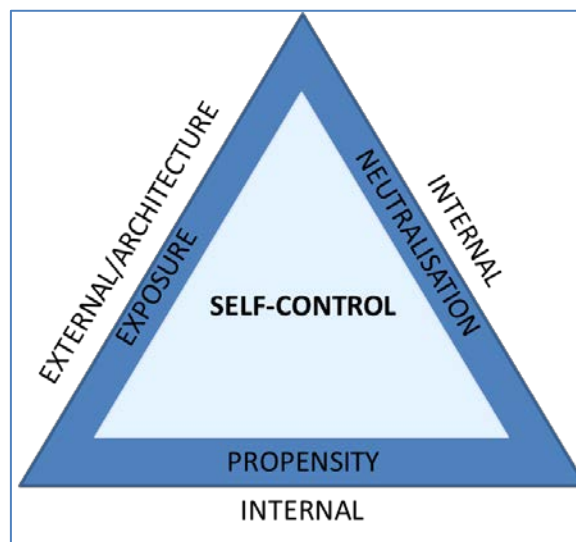
The propensity variable in SAT was used in SAT-RI as the set of moral rules pertaining to the individual. Also, the ideas of situational self-control will play the same fundamental part in SAT-RI it does in SAT (but connected to a different environment altogether). What is being proposed and explored in this thesis is that individuals have a specific propensity to the commission of cybercrimes, in general terms. Also, the SAT-RI explores the use of neutralisation techniques by individuals when committing cybercrimes in order to justify their actions.

The triptych that defines the SAT-RI would, therefore, be:

Individual Cybercrime Propensity (P) X Exposure (E) to the internet (understood as a criminogenic setting per se) x Neutralisation (N) techniques after a process of moral deliberation (mediated by self-control) might result in the commission of a specific cybercrime (CC) or **P x E x N=CC**.

Figure 6 summarises the SAT-RI elements. The Figure depicts cybercrime as the product of the concurrence of external and internal elements. The internal elements are cybercrime propensity, and the use of neutralisation techniques. The external element is the coming into contact with the internet. Finally, self-control mediates between the internal and external elements, as it does in SAT.

**Figure 6. The triangle of cybercrime**



## **2.4. Neutralisation Techniques**

### **2.4.1. Neutralisation techniques: Sykes and Matza**

The concept of neutralisation techniques was proposed by Sykes and Matza in 1957. The theory stems from the idea that “The difficulties in viewing delinquent behaviour as springing from a set of deviant values and norms ... are both empirical and theoretical” (Sykes & Matza, 1957, p. 664) and contradict (or, at least, steer away from) paradigms, such as Sutherland’s (as mentioned, for example, in Sutherland, 1983) that understand criminal subculture as acquired by social contagion.

As indicated by the Sykes and Matza (1957), “it is doubtful if many juvenile delinquents are totally immune from the demands for conformity made by the dominant social order”, p. 665) meaning that delinquents may ascribe their moral codes to conventional moral values, instead of deviant ones:

The juvenile delinquent would appear to be at least partially committed to the dominant social order in that he frequently exhibits guilt or shame when he violates its proscriptions, accords approval to certain conforming figures, and distinguishes between appropriate and inappropriate targets for his deviance. (Sykes & Matza, 1957, p. 666)

In order to cope with the moral conflict, the delinquent was able to develop justifications for his actions. Scripts that were able to rationalize what he/she had done and act, as indicated earlier, as “a protection from the self-blame and the blame of other after the act” (p.666).

These scripts were divided into five categories by Sykes and Matza (1957, pp. 667-669):

- a) Denial of Responsibility: where deviant acts were considered either accidents or resulting from exogenous overwhelming forces. In these cases, the delinquent must use a narrative such as “it is not my fault” or “it was them drugs” (for a very interesting account of personal retroactive narratives, see Maruna, 2001).
- b) Denial of Injury: in this case, the delinquent may justify him/herself by indicating that acts were not expressly prohibited and did not cause great harm. This is extremely important in terms of cybercrime, when for example, individuals claim that cyberbullying is just a mere prank or illegal downloading is justified because “it is not like it is stealing”.
- c) Denial of the Victim: whereby the delinquent may accept the blame, but justify that the injury is not real in relation to the victim, or even an act of retaliation. As Sykes and Matza (1957) reasoned “by a subtle alchemy the delinquent moves himself into the position of an avenger and the victim is transformed into a wrong-doer” (p. 668). Also, the victim can be vague or abstract. This is extremely relevant when talking about different cyberfrauds where the victim can be understood as guilty of being so greedy (as in Nigerian scams, for example, see Delio, 2002), or simply diffuse or inexistent.
- d) The Condemnation of the Condemners: in this case “the delinquent shifts the focus of attention from his own deviant acts to the motives and behavior of those who disapprove of his violation” (Sykes & Matza, 1957, p. 668). As an example, a student may have copied in an exam, but he/she justifies it because his/her teacher is an

extremely vile person who wanted all the class to fail. This can result in “bitter cynicism” (1957, p. 668) against establishments of social control such as the police, the education system of even parents.

- e) The Appeal to Higher Loyalties: the delinquent is conflicted as he or she is obliged to neutralise by “sacrificing the demands of the larger society for the demands of the smaller social groups to which the delinquent may belong such as the sibling pair, the gang, or the friendship clique” (Sykes & Matza, 1957, p. 669). In this case, the delinquent may refer to concepts such as the sense of “brotherhood” in order to neutralise the commission of anti-social acts. But also to concepts such as justice, fairness, religion, ethics or politics.

These were the five key types of neutralisation techniques mentioned by Sykes and Matza; however this is not the final list. Owing to the development of criminological science and the passing of time, new techniques have been added. These techniques are identified in the below discussions of the relationship between neutralisation techniques and cybercrime.

Syke and Matza’s theory was pioneering because it normalised the idea of delinquency. Before, in positive criminology, the delinquent is viewed as a “monster”, a genetic anomaly or a product of social malaise. However, Syke and Matza’s conception, of delinquents belonging to the same moral pool as non-delinquents contradicted the construction of the criminal as socially alien. The juvenile delinquent, following neutralisation theory, does not understand himself/herself as a delinquent. Criticism has, though, arisen recently in relation to this theory. Christensen (2010) argued that:



(1) Analysts using the neutralization concept construct an interpretive framework that frames the motives and desires of those being studied in a way that directs us toward interpreting speech as a neutralization; (2) By constructing people and actions in this way, analysts subtly 'take the side' of those who condemn the behavior in question; and (3) In applying the neutralization concept analysts engage in what Mills (1940) refers to as 'motive mongering'. (p. 554)

Christensen's study is very relevant for researchers, as they might feel tempted to mark mere explanations by offenders as neutralisation techniques. Also, by "mongering motives" he referred to researchers who "claim to have insight into why their subjects 'really' explained their behaviour in this manner" (Christensen, 2010, p.564). Christensen warns about the subjective interpretation of neutralisation techniques by researchers, and also about how researchers may act as agents of "conventional morality" (p. 570). This could happen if researchers use these techniques as a way of judging the individuals they are researching or the acts these individuals commit. However, this is not solely a thesis exploring how offenders use neutralisation techniques to justify their behaviour in light of conventional morality, but of how neutralisation techniques occur on the internet (conceived as a criminogenic setting in itself) and are also linked with the propensity variable in order to result in acts of crime online.

Also, it must be noted that, neutralisation techniques are extremely useful in understanding the commission of the majority of cybercrimes. Many cybercriminals will opt for the use of these techniques, stemming from the very architecture of cyberspace and the distance between the victim and the offender. On the internet, many crimes are not committed (or more important are not viewed as committed, as it is theorised) against a particular victim, due to the lack of social cues, personal presence and time-compression. On the other hand, not all cybercrimes are victimless (for example, cyberbullying), but offenders are able to justify

their offences owing to the distance between themselves and their victims. As mentioned above, the lack of social cues and the architecture of the internet allow the offender, at least, to act anonymously.

#### **2.4.2. Neutralisation techniques on the Internet**

There are numerous studies on the topics of cybercriminals and neutralisation techniques that would serve the purpose of exemplifying how the internet facilitates the use of said narratives and scripts. Delio (2002), in a feature in *Wired* magazine, quotes a Nigerian cybercriminal: "Others have come up with ways to justify it. They say Nko? (So what?). It is not our fault foreigners are so greedy." and "You would (be) shock(ed) at how many wad (rich people) want something more for nothing". There is, in this feature, a very clear example of the script: denial of victim. The victim becomes even guiltier than the criminal, in fact all the blame is placed on his/her greed (the whites' greed, the foreigner's greed). It can even be seen as an act of just retaliation against "those greedy foreigners".

A study on hackers by Turgeman-Goldschmit (2011) discovered several narratives that can be incardinated within neutralisation techniques. Some hackers indicated that "it's the way to a better world, not letting companies like Microsoft control the market" (p. 39) and "much of my religious life still remains in me with respect to values. The fact that I've never committed a crime may be related to this. I'm a good boy, in whom the good side survived." (p. 39) or even "I see myself the state's guardian. If the government isn't doing anything, I feel I should, and I do something." (p. 41). Hackers did not see hacking as a crime, but as some quixotic crusade against dominant corporations and they recognise their ascription to conventional (and even religious) morality. What motivates them, according to Turgeman-Goldschmit, seems to be, in

general terms, the quest for prestige, thrill or technical challenge. In relation to online child pornography users, one study concluded that

Internet child pornography consumers may understand that engaging in this behavior is socially illegal, but they may not believe that it is 'wrong' for them personally, compared with non-child pornography users who believe it is morally wrong both at the social and the individual level. (Seigfried-Spellar, Lovely, & Rogers, 2011, p. 74)

This is because, as the authors indicated "a person's internal values are not determined by society's laws or regulations but are instead a private, moral choice" (p.74.) Thus, offenders might understand that some action is regulated as a crime or is simply considered morally wrong, but that these rules do not apply to them personally. In Seigfried-Spellar et al.'s study, child pornography consumers understood their actions as illegal but they decided to engage in them no matter what.

Neutralisation techniques have also been examined in the context of studies of internet-based music piracy. Higgins, Wolfe, and Marcum (2011), for example, explain that "the findings of the present study indicated that individuals will take a 'holiday' from social controls to allow themselves to pirate music without developing a pirating identity" (p. 204) and concluded that "Participants in music piracy are often misguided about their perceptions of the harm that is caused through participation in this behavior—as well as the responsibility that resides with them" (p.205). In regards to digital file sharing, Moore (2011) mentioned the use of more neutralisation techniques already discussed by scholars: "The metaphor of the ledger whereby an individual argues that unacceptable behavior was acceptable because the person had built up a reserve of good deeds" (Moore, 2011, p. 214, citing Klockars, 1974) and "Coleman (1994) proposed three additional neutralization techniques: denial of the necessity of the law, the claim that 'everybody else is doing it', and the claim of entitlement" (Moore, 2011, p. 214).

Finally, “Minor (1981) also proposed an additional neutralization technique known as the defense of necessity: this technique claims that although an individual’s behavior may be inappropriate, it was necessary in order to prevent an even greater criminal or delinquent act.” (Moore, 2011, p. 215). These newer developments of neutralisation techniques did not contradict the five mentioned by Sykes and Matza (1957) but completed the catalogue with variations on the classical ones (although they can easily fit as sub-categories of the five key techniques). Moore (2011) continued by indicating that “Participants in this study provided evidence of the use of 6 of the 10 techniques of neutralization when justifying their digital file-sharing behaviors.” (p. 216). To summarise, the complete list of neutralisation techniques that occur in cybercrimes are, according to literature, as follows:

- a) Denial of Responsibility
- b) Denial of Injury
- c) Denial of the Victim
- d) The Condemnation of the Condemners
- e) The Appeal to Higher Loyalties
- f) The metaphor of the ledger
- g) Denial of the necessity of the law
- h) Claim of entitlement
- i) Everyone else is doing it
- j) Defense of necessity

Some interesting examples from participants in Moore's (2011) study are:

Recording artists are not victimized by this type of activity. I only download music CDs from artists who are no longer a part of the top 100. These individuals aren't selling CDs anymore, so they are not harmed when I download their music. (p. 218)

And,

Almost everyone I know downloads music. If it were truly wrong then why would so many people be allowed to get away with it?... I pay my monthly Internet bill. Whatever I can get for \$29.95 is what I believe that I have a right to download. It may be illegal, but it shouldn't be available to me if they don't want me to have it. (pp. 119-220)

Hinduja has also studied neutralisation techniques empirically in regards to music piracy (Hinduja, 2007; Ingram & Hinduja, 2008). He also mentioned a more comprehensive catalogue of neutralisation techniques including the "the metaphor of the ledger" or the claim of normalcy (Hinduja, 2007, p. 190). He reminded readers that "these nine techniques of neutralization are utilized by individuals to be freed from moral, ethical, and legal bindings and to rationalize participation in some form of wrongdoing." (2007, p. 190) and concluded that "In the current work – and consonant with previous studies – respondents generally did not view software piracy as morally reprehensible. This may be the reason that only four out of nine neutralization techniques were significantly related to the criterion measure" (Hinduja, 2007, p. 197). Another study of university students and illegal downloading of music, carried out by Ingram and Hinduja (2008), seemed to validate the aforementioned affirmations: "the findings suggest that neutralization theory can be a useful framework for understanding online piracy and bear important policy and theoretical implications for efforts to address this behavior,

especially Neutralizing Music Piracy within university settings” (pp. 357-358). More specifically, they pointed out that:

The results indicated that greater acceptance of the techniques associated with denial of responsibility, denial of injury, denial of victim, and appeals to higher loyalty were significant predictors of moderate levels of piracy participation (e.g., downloading 101-1,000 MP3s). Greater acceptance of these techniques substantially increased the probabilities of moderate participation. Furthermore, greater acceptance of the higher loyalty technique was also a significant predictor of high participation levels (e.g., downloading >1,000 MP3s). (Ingram & Hinduja, 2008, p. 356)

Also, a study by Moore and McMullan (2009) on Digital Piracy concluded that:

the individuals who utilize P2P file sharing software may be completely law-abiding citizens on every level except for when it comes to downloading music and movies from P2P networks ... these relatively law-abiding citizens may consider no longer downloading or utilizing P2P networks if they were more certain of the likelihood of their being caught and charged with a criminal or civil offense. (p. 449)

The internet has become the perfect environment for the usage of neutralisation techniques. Victims are removed from sight, fuzzy, abstract or quasi-nonexistent; cyber-fraudsters do not know who will contact them or do not tailor scams to specific people (with the exception of “spear phishing” a newer form of phishing designed for a specific user, see Wall (2013, p. 439)). As discussed previously, in some other cases companies may be victims of crimes such as hacking or online piracy. In these situations, offenders view themselves as heroes, fighting against dominant and shady mega-corporations. Overall, illegal downloading seems to be the crime that offers the richest catalogue of techniques, especially those involving the absence of

a “real crime”: “I’m not doing anything wrong, it’s not like I am killing someone” or the claim of normalcy: “everyone is doing it”.

It is theorised, in this thesis, that neutralisation techniques are so profoundly embedded in the fabric of internet crime that they have become a prominent feature of it. The architecture of the internet facilitates the use of many neutralisation techniques for all the reasons that have been mentioned in earlier paragraphs (anonymity, global reach, asynchrony, infinity, absence of capable guardians, eternity, as examples.). It is also theorised that these techniques are used in all types of cybercrimes, be they violent, sexual or economic in nature.

## **2.5. Summary of SAT-RI and Research Questions**

As has been discussed through this chapter, the aim of this study is to update existing criminological theory in order to explain the commission of cybercrimes. In order to do so, Wikström’s SAT essential formulation (propensity x exposure mediated by self-control= crime) is updated into what has been named SAT-RI, by adding neutralisation techniques to the propensity x exposure x neutralisation techniques mediated by self-control= cybercrime).

Also, SAT-RI is theorised under the following postulates:

- 1) It is a theory that serves as an explanation of cybercrimes only (albeit all types of cybercrime).
- 2) It operates under a broader definition of cybercrime, which was presented in this chapter, and includes deviant cyberbehaviour.
- 3) It considers that the mere exposure to the internet is criminogenic in itself, therefore exposure will be treated as constant (in the propensity x exposure x neutralisation model). On the other hand, self-control, cybercrime propensity and the use of neutralisation techniques are going to be measured.
- 4) It does not pay attention to the device the internet is accessed from (computers, wearables and smart phones, for example).
- 5) It considers the whole of the internet as the setting and does not make any distinctions as to whether the user is accessing the surface internet or the darknet (or deep web).
- 6) It tries to consider the impact of the advent of digital technologies on human nature, behaviour and identity.



The research questions (RQ) formulated are:

RQ1. What is the role of self-control in cybercrime causation?

RQ2. What is the role of personal propensity (morality and engagement) in cybercrime causation?

RQ3. What is the role of neutralisation techniques on cybercrime causation?

RQ4. What is the relationship between morality, self-control and neutralisation techniques in cybercrime causation?

RQ5. What are the general population's views and attitudes towards cybercrime?

RQ6. How do law enforcement agents investigate and tackle the issue of cybercrime and cybercriminals?

## **Chapter 3: Methodology**

### **3.1. Aims and Objectives**

The main objectives of this study were to explain why people commit cybercrimes and how they are able to cope with the consequences of online rule-breaking activities and to upgrade criminological theory relation to the still relatively new, and developing, phenomenon of cybercrime.

The original SAT, developed by Per-Olof Wikström (Wikström et al., 2013) is a moral-based crime theory that understands crime as being a result of process of moral deliberation. This process takes into consideration the criminal propensity of the deliberator and the moral rules of the environment. Both variables (exposure and the propensity) are moderated by the idea of self-control, which is conceived as a situational concept, depending on the intersection between environment (external variable) and moral structure of the would-be offender (internal variable), rather than the static personality trait theorised by Gottfredson and Hirschi (1990); a trait that develops in infancy and becomes fixated at a certain age.

As discussed above, cybercrime is a novel and mutating phenomenon, and one that is very difficult to explain with current criminological theory, as it involves interactions that differ profoundly from those happening in “real life”. SAT theory is able to explain this situational concept (the coming together of personal traits and environmental traits) up to a point, as both variables exist when committing cybercrimes. Propensity refers to the tendency of the agent to engage in different acts of cybercrime (understood as a new species of crime rather than a specialty of traditional forms of crime), whereas exposure takes for granted that contact

with the internet is criminogenic to some extent. As explained in the literature review, criminogenic places attract and generate crime (Wikström et al., 2013). After having studied current literature on cybercrime and its different manifestations, one recurring idea appeared fundamental: neutralisation techniques. Research provides a rich catalogue of cognitive scripts that are used by cyber-criminals to protect themselves from their own blame or the blame of others. This is the reason why Situational Action Theory-Revised for the Internet (SAT-RI) was formulated; to explain that cybercrime is the result of a moral process of deliberation that results from the relationship between the individual's own criminal propensity, the exposure to a criminogenic setting (that is taken for granted, as the internet was considered as criminogenic in itself for this study) and the application of a successful neutralisation technique.

The following methodology tested this relationship, between propensity, exposure and neutralisation techniques, and it also sought to ascertain the general amount of self-control the sample exhibited. In addition, it endeavoured to understand which neutralisation techniques are used by cybercriminals.

The general objectives (GO) of this thesis are:

GO1. The updating of criminological theory

GO2. The understanding of the aetiology of cybercrime

Specific objectives (SO), on the other hand, are:

SO1. To test the proposed SAT-RI theory by using mixed methods research

SO2. To understand the role of self-control, propensity and neutralisations in cyber-crime causation

SO3. To understand the motivations and justifications behind the behaviours of individuals committing cyber-crime

SO4. To study how cybercrime is investigated and how cybercriminals are perceived by law enforcement agents

## **3.2. Research Approach**

### **3.2.1. A mixed methods study**

This work used mixed methods research, as defined by Creswell (2015):

An approach to research in the social, behavioral, and health sciences in which the investigator gathers both quantitative (closed-ended) and qualitative (open-ended) data, integrates the two, and then draws interpretations based on the combined strengths of both sets of data to understand research problems. (p.2)

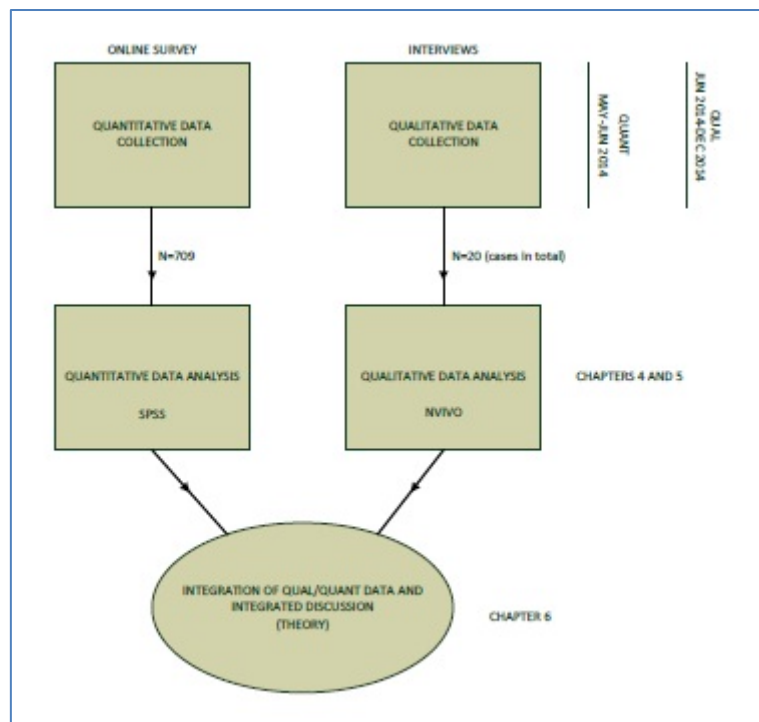
Testing a theory usually implies a more positivistic approach based on the use of quantitative research methods (Gibbs, 2014). In relation to this, a part of the SAT-RI can be measured using scales (for example, self-control) but other elements (like perceptions of morality or the use of neutralisation techniques) are based on subjective realities. Although that inherent subjectivity was also numerically measured, via an online survey, there was a need “to hear the voices” of the cybercriminals (or at least, those committed to investigating and pursuing them). Following that approach, a broader understanding of the cybercrime phenomenon could be obtained. According to Creswell (2015), the use of mixed methods can be useful “when the use of quantitative research or qualitative research alone is insufficient for gaining an understanding of the problem” (p.14). The main reason for using mixed methods in this study was to measure the variables of the SAT-RI formula: cybercrime propensity, neutralisation and self-control. A quantitative approach was more suited for measuring self-control by using a scale. On the other hand, as cybercrime propensity and neutralisations relate to perceptions and behaviours, quantitative and qualitative approaches complemented each other.

In terms of the design, and following Creswell's (2015) categorization, the researcher opted for a convergent design: one that implies a parallel use of methodologies (not only in terms of time and space) but in this case in terms of testing a new theory. That is the reason why, in some instances, the qualitative and quantitative data collection took place simultaneously (for example, during June 2014 some interviews were carried out and the online survey was still available via social networks). In addition, three different analyses and discussions took place during the study: one dedicated to analysing the quantitative results using statistical tests, another one dedicated to analysing the qualitative results, including a discourse analysis; and finally, one last chapter dedicated to integrating both "strands of data" (Creswell, 2015), not by simply comparing or juxtaposing them, but by applying them to the proposed theoretical framework (SAT-RI). According to Leech and Onwuegbuzie's (2009) classification, the study at hand could be classified as a "partially mixed concurrent equal status design":

A partially mixed concurrent equal status design involves conducting a study that has two phases that occur concurrently such that the quantitative and qualitative phases have approximately equal weight. (Leech & Onwuegbuzie, p. 268)

The SAT-RI data was obtained from different sources, not in an absolutely simultaneous manner, as the quantitative data was collected during May 2014 and June 2014, whereas the qualitative data collection started in June 2014 and finished in December 2014. After being discussed separately in two different chapters (Chapters 4 and 5), both strands of data were finally integrated (Chapter 6). Both strands of data aimed to test the theory from different and complimentary angles. Chapter 6 also served to answer the research questions and relate the findings from Chapters 4 and 5 to the formulation of the SAT-RI from the Literature Review (Chapter 2). This methodological design is explained in Figure 7.

**Figure 7. Diagram of the mixed methods design of the SAT-RI study**



The core of the research was to demonstrate the aforementioned co-existence of neutralisation techniques (as used in respect of internet crime) and personal traits conducive to the commission of online crimes. In addition to this, self-control was considered as the arbiter in between the inner world of the offender and his/her external reality. The external variable (the architecture of the internet as a criminogenic setting) was not measured - given that, as explained in previous paragraphs, the internet will be assumed as a criminogenic setting – in accordance with current literature. In other words, this work aims to measure the variables propensity, self-control and neutralisation techniques in relation to cybercrimes. In order to do that, an online survey was designed and administered, containing a self-control scale and a series of vignettes that aimed to understand participants' propensity towards cybercrime and their use of neutralisation techniques. Also, interviews with law enforcement agents were carried out to provide information (in the form of case studies) about the

motivations and justifications of offenders, as perceived by police officers, and the manifestations of cybercrime in Spain.

Having said this, it has to be borne in mind that this work related to the perceptions of offenders or potential offenders; neutralisation techniques, propensity and self-control are, therefore, subjective constructs. Neutralisation techniques are cognitive scripts, protecting oneself from self-blame and the blame of others, whereas propensity refers to the moral compass of the offender and its flexible interaction with the environment. Self-control, as the ability to postpone satisfaction and pleasure depending on the situation, is also embedded in the subjectivity of the individual's narrative. All of concepts called for a subjective approach, a "hearing of the voices" of cybercriminals and the general public in relation to cybercrime, and at the same time, a (theoretically) more objective approach: the testing of a theory by using quantifiable variables. This is the reason why a convergent mixed methods study was judged to be better suited for addressing the general and specific objectives of the study, as well as answering the research questions. Both the quantitative and qualitative strands relate to perceptions and subjective constructions of the world or personal traits (for example, self-control). This is one of the reasons why the study is not epistemologically conflicting and why a threefold analysis of the data was performed: the analysis and discussion of quantitative data, the analysis and discussion of qualitative data, and the integration, analysis and discussion of both strands.

The approach chosen for this research was one that was indirect, testimonial and online-based. The use of "second-hand" (testimony) knowledge became fundamental to the interviews, as the researcher tried to understand the perceptions of cybercriminals by using police officers as "proxies" for them. The researcher assumed that (specialised) police officers



would be a valuable source of data and that the nature of their work would place them in an advantageous position for accessing the world of the cybercriminal, as they investigate cybercrime as part of their job. The possible existence of a police culture (Reiner, 2010), a police discourse and an ideological standpoint had to be addressed. The police interview chapter (Chapter 5) dealt with all these issues and provided a narrative analysis of data stemming from police interviews. Also, Chapter 6 approached the reality of the possible existence of a police discourse.

Several police officers, from different Corps and Units, were invited to take part in interviews. Individuals working for the private sector were also invited to take part in interviews, in order that a wider picture of cybercrime and cybercriminals could be obtained. In relation to law enforcement agencies, access is a very complex issue in Spain. Access was negotiated for almost two years. Guardia Civil and Private Security experts were very eager to collaborate. However, Spanish National Police has a very opaque structure in terms of relations with academia. After two years of correspondence through formal channels an opportunity to gain access to a police gatekeeper arose.

As indicated before, the research approach was indirect, testimonial and online-based. By indirect, it is meant that the research methods used (in this case the online questionnaire) were not used to measure actual offender's points of view but the general population's views on morality and cyber-offending. Projective (indirect questioning) techniques are very common in marketing and other social sciences (Fisher, 1993) and thanks to the use of snowballing, via social networks; they can offer a very interesting view on how cybercrime is perceived by internet users in Spain. Some of the respondents will have committed one or more of the cybercrimes depicted in the scenarios, while others will not have done so.

However, this will hold no relevance to the study, as what will be taken into consideration is the relationship between the variables morality (perception of), self-control and neutralisation.

Finally, the questionnaires were administered online. There were no hard copies of the questionnaires and they were posted in different social networks (Twitter, Facebook, Google+ and LinkedIn) in order to be snowballed. That way, the researcher was able to reach as many respondents as possible, as the only pre-requisite for answering was having access to the internet. In addition, one of the advantages of online administration was that processing and analysing data was quicker and easier.

### **3.2.2. Epistemology**

Summarising, the fundamental aims of the study were to:

1. Develop existing theory – SAT- to better explain cybercrime
2. Explain attitudes among both the “general public” and offenders towards cybercrime

The present study used a mixed methods approach that integrated qualitative and quantitative data under a convergent design where both strands tended to have equal weight. The quantitative data represented morality, self-control and neutralisations among a sample of internet users, whilst the qualitative data originated from law enforcement agents, serving as proxies for the “worlds” of the cybercriminal.

Usually, deductive approaches tend to be linked to an essentially positivistic epistemology and quantitative methodologies (Gibbs, 2014). In contrast, qualitative methodologies (like the interviews with law enforcement agents) tend to relate to inductive approaches and interpretivistic epistemologies (Gibbs, 2014). However, and following Bryman's (2012) discussion on mixed methodologies, Gibbs (2014) recognised that researchers often collect data that "span those philosophies".

These are the main epistemological issues that arise in mixed methods research: the opposition between quantitative and qualitative approaches. Bryman (2012, pp. 613-652) and Creswell (2011, pp. 269-283) talk about controversies in mixed method research or the quantitative/qualitative divide. Creswell discussed the idea of "bilingual" research (Creswell, p. 278). Similarly, Bryman elaborates how the distinction between quantitative and qualitative can be understood as somewhat artificial and how quantitative research can be understood from a qualitative standpoint and vice-versa (2012, pp. 619-626).

As shown in the outline of the research design in Figure 7, the quantitative data collection started before the qualitative data collection, yet both were run simultaneously for a period of time. This did not indicate a hierarchy between the two stages. Both the survey data and the interview data were discussed separately in different chapters and finally integrated in an overall analysis and testing of the theory.

The idea of theory testing, points to the fact, epistemologically, that the present work is mostly positivistic, employing deductive approaches. In contrast, and following Bryman's (2012) discourse on the "divide" (pp. 614-626), this chapter has elaborated a methodology that is

more in tune with qualitative research methods. Or at least, qualitative methods in a “quantitative carcass”.

First, the self-control scale and the vignettes were instruments used to measure attitudes. Even though they were presented in a numeric fashion, the use of Likert scales, artificial scenarios (vignettes) and more importantly the use of variables, such as morality or neutralisation techniques, demonstrate a powerful qualitative inclination. Respondents were not asked about how many days a week they use the internet or whether or not they view online pornography. They were asked about how they rate themselves in attitudinal scales, or whether they perceive certain situations as moral or immoral. This qualitative approach, in a “quantitative carcass”, permitted the creation of a much bigger sample and profited the viral capabilities of the internet.

Secondly, interviews related to the perceptions of police officers about the motivations and justifications of offenders. By following “the proxy approach” an insight into police culture was obtained. It must be strongly affirmed that this is not a cultural study, but certain elements of police culture might have been interwoven with the interviews. How do police officers construct the idea of the criminal? How do they ascribe moral judgement to them? Is the cybercriminal a real entity in itself or is it a narrative designed by a common cultural framework? Are interviewees talking from ‘their own experience’ or the ‘collective corps experience’? This called for extreme care at the data analysis phase of the study, as a critical approach to what is being said or taken for granted was also necessary.

In summary, the study at hand used a deductive approach in order to test new criminological theory. In order to do so, a mixed methods study design was used. Although, the study comprised a quantitative stage (adhering to positivism) and a qualitative stage (adhering to interpretivism), the underlying spirit of the study was qualitative and called for a more critical interpretivistic epistemology.

### **3.2.2. PADS+ as a methodological example of applying SAT**

In order to measure self-control and propensity, and test SAT longitudinally, Wikström et al. (2013), via PADS+, used an approach that offered post-hoc validation of some of the methodological decisions in this thesis, albeit with some differences. It must be borne in mind that the design of the methodology of this study was carried out before the publication of the PADS+.

In order to measure crime propensity, the PADS+ used a generalized morality scale (p. 132) asking participants to rate the wrongfulness of several items (depicting actions) measured with Likert scales from 0 to 3 (being 0 nothing wrong at all and 3 very wrong). On the other hand, in order to measure self-control the PADS+ used a modified version the Grasmick, Tittle, Bursik, and Arneklev (1993) self-control matrix using only eight of the twenty four original items (pp-135-137).

The decision to use the self-control matrix designed by Grasmick et al. (1993), in order to develop Gottfredson and Hirschi's (1990) self-control theory, both in the PADS+ and the SAT-RI, should be explained. As has been shown above, Wikström's SAT's vision of self-control is

situational, whereas Gottfredson and Hirschi's self-control is understood as static by the authors. Grasmick et al. (1993) indicated when talking about Gottfredson and Hirschi's work "their focus is on early childhood socialization in the family, which can produce an enduring criminal predisposition called low self-control" (p. 6). In other words, once low self-control is developed, it becomes fixated as a personality trait. Contrarily, Wikström et al. (2013) theorised that "a person's *ability to exercise self-control* only comes into play when the moral norms of the setting encourage him or her to break a rule of conduct but his or her moral rules discourage doing so in response to a motivation" (p.26) and:

A person's ability to exercise self-control depends on his or her executive functions (general cognitive abilities) but also on temporary personal factors like intoxication or extreme stress or emotion (Wikström et al. 2013, p. 28; citing Wikström & Treiber, 2007)

Therefore, within SAT, self-control is situational. However, when explaining the use of the modified Grasmick scale for the PADS+ there was some recognition of the stability of low self-control through age (taking into consideration that the study focused on young people) and the possibility of self-control having a genetic component is considered (Wikström et al., 2013, p. 137).

Crime propensity was measured by merging the z-scores of the scales of "weak morality and poor self-control" (p. 137) thus creating a "composite measure" (p. 137). Participants were then divided into groups of low, medium and high crime propensity for analysis. This division was performed by using the means of crime propensity; according to the authors "these are, of course, somewhat arbitrary cut-off points" (p. 139) but illustrative of the differences between low, medium and high propensity, nonetheless.

Finally, scenarios were used in the PADS+ in order to test how participants would act “if they were the protagonists in specific hypothetical scenarios” (p. 367). The researchers in the PADS+ aimed for clarity in the scenarios, but also for familiarity and realism (pp. 370-373) for adolescents growing up in the UK. One of the key features of the scenario approach – and one that was fundamental in the present study - is, according to Wikström et al., that “it is plausible for participants to form judgements about how they would act in situations they have never encountered by applying attitudes to, and past experiences of, familiar situations” (p. 371).

### **3.3. Online Survey on Attitudes Towards Cybercrime**

The questionnaire (see Annex 1) was designed and stored via Google Drive and consists of three parts. The questionnaire survey was launched on the 24<sup>th</sup> May 2014 and was closed on 10<sup>th</sup> June 2014. It was uploaded into the researcher’s personal accounts on the following social networks: Twitter, Facebook, LinkedIn and Google+.

Before being administered in the main study, the questionnaire was piloted on four occasions with the same group of ten people that comprised students from several universities, lecturers and lawyers, and friends who had no professional interest in criminology. Their comments on clarity, wording and timing were extremely helpful and were incorporated into the questionnaire. One of the most important comments related to perspective, as some of the piloting respondents were confused as to the point of view from which they should answer the vignettes. This resulted in the following line being added to all the neutralisation questions: “In the case of doing it (place yourself in Jill’s shoes)” (as an example from the illegal downloading

case questions) also, in the morality and engagement questions the researcher asked participants about the wrongfulness of the acts a specific character had performed or if they would engage in behaviour similar to that of a specific character. Following the illegal downloading example, respondents were asked: “Would you do what Jill did?” and “How morally wrong do you think Jill’s actions are?”. The first question aimed to measure (by using a Likert scale) whether or not respondents would engage in the acts depicted in the scenario (the engagement variable), whilst the second one aimed to measure the perception of morality of the act (also using a Likert scale). Both variables (engagement and morality) are part of cybercrime propensity. The piloting also discovered some spelling mistakes that were corrected. It also demonstrated that the survey took much less time to fill in than it was anticipated (less than 20 minutes).

### **3.3.1. Sample**

The questionnaire was posted in four social networks with the intention of obtaining as large a sample of internet users as possible. The sampling, therefore, was a non-probability sample (Bryman, 2012, pp. 201-204) by snowballing and it did not follow any randomisation procedure. The idea was for it to expand organically through the social networking sites. Whoever wanted to open the link and answer the survey questions was able to do it without any restrictions. Bryman (2012) mentions the difficulties of using probability sampling on the internet (p. 674). In addition to the sampling issues mentioned, according to Hooley, Marriott, and Wellens (2012):

The key sampling issues are, however, whether the population that can be accessed using an online survey is different to that which can be reached using other survey approaches (sample bias), and whether respondents behave in a different way because



they are participating online as compared to another survey method (measurement error) (Hooley, Marriott, & Wellens, 2012, p. 43)

Yet Hooley et al. (2012) invite researchers to “to continue to innovate in the methodologies that they use in order to continue to address and respond to these changes” (p. 43). The use of an online survey seemed to be intertwined with the idea of accessing internet users in order to gather data.

At the very same time, access to the researcher’s colleagues’ classes was negotiated, as another means of administering the online survey that had previously been uploaded into MOODLE (Virtual Campus). Six classes were finally approached (three from the Criminology Degree and three from Law). Students were informed as to the aims of the research and all other aspects of the study, in person, by the researcher. Students ranged from Year 1 to Year 4 students<sup>11</sup>. In the end, a sample of N= 709 respondents was obtained.

One of the most important characteristics of the sample, in terms of measuring propensity and self-control, was that internet access was needed. According to official Spanish statistics from the *Instituto Nacional de Estadística* (INE, National Statistics Institute), 96.2 % of people who have used internet at least once a week in the last three months are aged 16-24 years, whereas 89.9% percent of individuals who have used internet at least once a week in the last three months are 25-34 years of age (INE, 2015a). Also, 98.2 % of the users who have used the Internet at least once a week in the last three months are students (it is not specified whether they are school and/or university students) (INE, 2015c).

---

<sup>11</sup> The Criminology and Law Degrees at Universidad Europea de Madrid are four-years degrees

Having said that, in relation to the questionnaire, the following sampling procedures were followed:

- Captive audiences: the researcher used several classes from the Universidad Europea de Madrid, in order to solve eventual response ratio issues<sup>12</sup> that might have arisen during the online survey; respondents were used from his students and whole classes were asked to complete the questionnaires; and no discrimination between bachelor students, in terms of the subject they were studying, was going to be made at first but the researcher failed to gain access to students from disciplines other than law and criminology. This sample was expected to have an estimated size of 200-300. Students at this (private) university have a similar economic and cultural background to one another and this might have created a discrete socio-demographic. Private universities in Spain do not receive public funding; therefore enrolment fees are much higher. In addition, Universidad Europea de Madrid ranks as one of the most expensive universities in Spain. The sample is, therefore, probably unrepresentative, in terms of sociodemographic characteristics, of university students and young adults more generally in Spain (not to mention the general population). It is likely that the sample was made up of, for example, a disproportionate number of, affluent individuals and those who had an upper-middle class upbringing.
- Snowball online sampling: in order to obtain a bigger sample, the questionnaires were distributed via Facebook, LinkedIn, Twitter and Google+. The researcher is very active in social networks and asked followers and contacts to answer the questionnaire and share it. This helped the snowball effect due to the viral nature of information travelling through social networks. Also, the study was distributed via the Universidad

---

<sup>12</sup> These issues could mean individuals deciding not to take part in an online survey posted in social networks, they might not feel entirely comfortable with answering some questions by using an internet questionnaire or they might forget to answer if not reminded in person.

Europea de Madrid MOODLE (online platform) to other lecturers in order for them to use with their students and/social networks. A total sample of N=709 was obtained (including those respondents from captive audiences).

One could also argue that there occurred selection bias because of the lack of randomization procedures, the majority of respondents are related to the researcher's profession or field of studies and are part of collectives that are deemed to have specific cultural standpoints regarding, for example, police culture.

### **3.3.2. Instrument**

#### **3.3.2.1. Information, consent and demographics**

The first part of the questionnaire comprised an information and consent form for the respondents with all the necessary background information about the study including the ethical procedures that would be followed and the researcher's contact details. No signature was required for the consent form. Respondents were, instead, asked to tick different boxes indicating that they had read and understood each of the different aspects of the consent and information form. If respondents did not complete the tick boxes, then they could not continue to the questionnaire. They also had the option, at any time, to close the webpage without submitting any information. The respondents were informed of the possibility of withdrawing consent at any time and the necessity of ticking the boxes, should they wish to proceed to the questionnaire, was explained to them. In order to ensure participants received the most adequate and appropriate information, the researcher used the University of Huddersfield's set of standard project information sheets available and translated them into

Spanish, after adapting the content to the present study. This meant that participants were sufficient aware of the ethical procedures to be utilised in the research, such as informed consent and their right to withdraw. . This initial section of the questionnaire also addressed the issues of anonymity and confidentiality, which are guaranteed by the architecture of the Google Drive questionnaire facility. Moreover, Google Drive questionnaires store information automatically as a data-sheet in the Google Drive cloud service that can be accessed only by a combination of user name and password. These data-sheets contained no participant identification information, with the exception of demographics (for example, age and occupation). Google Drive added a timestamp to every line of answers indicating the exact day and time they were submitted. These timestamps were deleted when uploading the data-sheet into SPSS.

In terms of demographic data on the questionnaire, the following information was collected: gender, nationality, occupation and whether the participant (or someone close to him or her) had been a victim of crime or not in the last year. In terms of nationality, the variable was disregarded given the lack of representativeness of the non-Spanish population. Occupations were codified following a selection of the International Standard Classification of Occupations (ISCO-08, from the International Labour Organization (ILO)) groups and sub-groups (ILO, 2004). Finally, in terms of demographic information, the “victim of crime” variable was derived from the question: “Have you (or someone from your kin or close acquaintances) been a victim of or subject to a crime (in any of its manifestations or forms) in the last year?” The rationale for this question was to facilitate an analysis as to whether or not people who have been victimized or have people close to them who have been victimised had a different perception of the morality or immorality relating to cybercrimes or different levels of self-control.

### **3.3.2.2. Self-control scale**

The second part of the questionnaire consisted of a self-control matrix, as developed by Grasmick et al. (1993). This scale aims to measure Gottfredson and Hirschi's self-control by taking into account the elements of the construct identified by the authors and developing a matrix of questions with different items. The following are the six elements of low self-control (Gottfredson & Hirschi, 1990, pp. 89-91):

- 1) A here and now orientation: impulsivity (as opposed to the capacity of deferring pleasure and satisfaction)
- 2) Preference for simple tasks
- 3) Risk-seeking
- 4) Preference for physical activity
- 5) Self-centeredness
- 6) Minimal tolerance for frustration and inability to respond to conflict verbally rather than physically

The Grasmick scale contained four items per element (i.e. 24 items in total) and all questions can be answered with:

- (1) Strongly Disagree
- (2) Disagree Somewhat
- (3) Agree Somewhat
- (4) Strongly Agree

High scores (3 or 4) indicate low self-control. This is extremely important; as questions in the original scale are formulated as indicators of low self-control (not of high-self-control) (e.g. “I often act on the spur of the moment”). Respondents that are in agreement with the items of the scale (those who had picked 3 or 4 as responses) had lower levels of self-control as they would agree to being impatient and self-centred individuals with a low tolerance for frustration, risk-seeking tendencies and a liking for physical activities (rather than mental ones) and simple tasks (rather than complex ones) (Grasmick, Tittle, Bursik, & Arneklev, 1993). Following Grasmick et al. (1993) “A high score, therefore, indicates low self-control” (p. 16). Table 2 is an example of the type of questions contained in the Grasmick scale.

**Table 2. Impulsivity items (Grasmick et al., 1993, p.14)**

Item	Mean	SD	Factor Loading
Impulsivity			
I often act on the spur of the moment without stopping to think.	2.53	0.97	.470
I don't devote much thought and effort to preparing for the future.	1.80	0.84	.388
I often do whatever brings me pleasure here and now, even at the cost of some distant goal.	2.06	0.91	.616
I'm more concerned with what happens to me in the short run than in the long run.	1.92	0.94	.580

In order to use the scale in Spain, Universidad Santiago de Compostela was contacted and the researcher was given a translation of the scale that had been piloted and tested by Romero, Gómez-Fraguela, Luengo, and Sobral (2003). This scale had been used in several Spanish studies and was translated following academic procedures designed to guarantee reliability and validity (see Carou, Romero, & Luengo, 2013). The order of the Grasmick questions was changed by Romero et al. (2003) and that exact same Spanish questionnaire (same wording and question order) was used in this study (See Annex 1). According to Romero et al. (2003) “The scales were translated to Spanish by two translators who translated the items independently, then compared results and negotiated complete agreement” (p. 65).

### **3.3.2.3. Cybercrime vignettes**

The third part of the questionnaire consisted of several cases (vignettes) in which the respondent was invited to consider several situations involving cybercrime. These vignettes were another means by which the researcher was able to assess individuals' propensity and their use of neutralisation techniques.

Given that morality is a critical feature within SAT, it is important to measure baseline morality in relation to cybercrime. The above vignettes were based upon those used by Schoepfer and Piquero's (2006) in their study of morality and self-control. They used scenarios depicting actions that could be considered morally reproachable and criminal (one, for example, involving a pub brawl and another one about a student stealing batteries) and "after reading each scenario, respondents were asked to estimate the likelihood that they would behave as the character in the scenario had acted" (Schoepfer & Piquero, 2006, p. 59). This was incorporated in the SAT-RI study, as the "engagement variable" and was measured likewise using a 0-10 Likert scale. Actions were presented in a way young adults (university students, for example) could relate to. Wikström et al. (2013) also used vignettes to assess decision making processes, in their case those of adolescents and young adults.

In order to import Schoepfer and Piquero's (2006) methods into this present study, seven vignettes were designed, each representing a particular cybercrime. These vignettes were drafted in Spanish and translated into English in the subsequent data analysis stage.

The cybercrimes chosen for the vignettes were those considered by the researcher to be crimes that the sample could most readily understand and relate to (especially, taking into consideration that the definition of cybercrime in this thesis includes crime and deviant behaviour). Online child abuse offences and hacking offences were deliberately omitted and left for the law enforcement interviews, as they are not frequently part of the general population's daily lives<sup>13</sup>. These scenarios tried to guarantee a high response rate and gather as much data as possible in order to form a clearer picture of general attitudes towards cybercrime.

Finally, the scenarios selected were:

- (1) Illegal downloading
- (2) Revenge porn<sup>14</sup>
- (3) Cyber-bullying
- (4) Sexting (in the vignette depicted as a minor sending erotic images to an adult)
- (5) Cyber-fraud (Russian bride)
- (6) Cyber-stalking
- (7) "Stealing" Wi-Fi signal

---

<sup>13</sup> Child abuse offences, for example, are likely committed by very few people whereas other offences e.g. illegally downloading music are much more common (and accessible).

<sup>14</sup> Misuse of erotic imagery by scorned romantic partners as punishment for break-up or infidelity (i.e. indiscriminate sharing and posting of photographs or sex videos).



The whole list of vignettes and questions can be found in Annex 2. The following, used as an explanatory example, is the illegal downloading vignette:

Jill wants to watch the recently released movie *The Wolverine*, but she prefers to stay at home, also the cinema is £6 which she finds very expensive. Jill decides to download a pirate copy of the movie and watch it at home

- a) Would you do what Jill did? 0-10 scale (being 0 absolutely disagree and 10 absolutely agree)
- b) How morally wrong do you think Jill's actions are? 0-10 scale (being 0 Not Immoral and 10 Absolutely Immoral)
- c) In the case of doing it (place yourself in Jill's shoes), what would you tell yourself or others to justify what you have done?
  - (1) It's not justifiable
  - (2) I haven't done anything wrong/I haven't committed any crime
  - (3) It's not my fault/It's someone else's fault
  - (4) It's the victim's fault (the person or company wronged by the crime)/He or she deserves it
  - (5) Everyone else is doing it
  - (6) I had no other choice
  - (7) It's my right to do so
  - (8) Nothing happens, if from time to time, I do something bad/wrong/illegal

In the sexting vignette, participants were asked to rate the case from the young girl's perspective, not the adult's. In the Spanish legal system, sending naked pictures of oneself is not a crime, even if the one sending them is a minor. This vignette was included on account that sexting is becoming a common practice and the researcher wanted to understand the

general population's views on sexting (Curnutt, 2012; INTECO & Orange, 2010; McAfee, 2014; Ringrose, Gill, Livingstone, & Harvey 2012). However, the definition of cybercrime used in this study does not only understand acts against criminal law as cybercrimes. In a study by the company McAfee:

Seventy percent of 18 - 24 year olds receive sexually suggestive content from someone.... More men are likely to use their mobile device to send and receive similar content (61% men vs. 48% women). Forty-five percent of U.S. adults say they stored intimate content that they have received in comparison to 40% who store risqué photos, videos or messages they have sent. Of those who have sent intimate or racy content, 77% have sent this content to their significant other, while 1 in 10 individuals have sent similar content to a total stranger (2014)

The above study used online questionnaires to collect data in the US and pointed towards a normalisation of sexting practices “while 98% of respondents use their mobile device to take photos, 54% send or receive intimate content” (McAfee, 2014). Ringrose, Gill, Livingstone, and Harvey (2012) carried out a study, in the UK, into sexting, for the National Society for the Prevention of Cruelty to Children (NSPCC). They found that digital technology had amplified the problem of sexting and that ever younger children were being affected (Ringrose, Gill, Livingstone, & Harvey, 2012, p. 8). It is evident that sexting has become a widespread practice amongst adults and it is starting to affect children (more children are sending indecent images, and more children are receiving them).

Going back to the vignettes used in the SAT-RI study, questions a) and b) (see previous pages) served as measures of propensity in a projective way (would I do something similar and would I rate it as morally wrong?) by using Likert scales. The first resulting variable was named “engagement”, whilst the second resulting variable was named “morality”. These two

variables “morality” and “engagement” were used to measure the propensity for the commission of cybercrimes.

Finally, question c) measured the variable neutralisation (seven different neutralisation techniques and one null choice were codified). It is important to indicate that question c) was a multiple choice answer, therefore the respondent could choose as many as he/she deemed necessary (from the eight that were available). In order to analyse data appropriately, with SPSS, each neutralisation technique was treated as a different variable. This produced a total of 56 variables. A further 8 neutralisation variables were coded, adding the prefix “SUM”, in order to measure total scores. Creating a “SUM” variable for each neutralisation technique allowed the researcher to understand which techniques had been chosen the most (from all the vignettes) and which techniques had been chosen the least. It also allowed the researcher to perform ANOVA’s with neutralisation techniques as the resulting SUM variables were categorical polytomous variables.

It was expected, during the design of the study, that the selection of the “unjustified” option would mean the exclusion of any other choice. In other words, theoretically, respondents that find actions unjustified should not need to use any neutralisation techniques. However, once the data were collected, two patterns that had not been anticipated by the researcher emerged: first, some respondents who picked the “unjustified” variable also chose other neutralisation techniques; secondly, some respondents did not pick any neutralisation techniques. This finding will be discussed in Chapter 4.

### 3.3.3. Procedure

The Internet is an integral part of this study, not only because the study tried to update criminological theory for the explanation of cybercrime but also because the study utilised specific features of internet architecture to execute the research. Currently, academics tend to differentiate between research “about the Internet” (it becomes the object of study) as opposed to research “with the Internet” (it is part of the data collection process) (Bryman, 2012; pp. 654-682; Hooley et al., 2012, p. 14). Research about the Internet could refer to content analysis (not only webpages but also social networks, such as Twitter, or user-created content like blogs or education platforms). As an example of this trend, in Spain, criminologist José Servera has published several blog articles on the study of the internet and social networks from a criminological perspective (Servera, 2014a, 2014b). In one article, he discusses the power of aggregated conceptual data from Twitter as a means of crime prevention (Servera, 2014a; citing Featherstone, 2013 and Gerber, 2014). In a second article, he discusses the paradigm shift that social networks have brought upon law enforcement (like Augmented Reality being used to analyse and prevent crime) and the challenges that new technological developments pose for the criminal justice system, society and criminology (Servera, 2014b). In relation to methods, Hooley et al. talk about a growing acquiescence between authors about the specialities of online research: “it is possible to construct a rationale ... for seeing online research methods as a field in its own right” (2012, p.15).

In the present study, the internet was both the object of study and the vehicle for the study. This is the reason why the current author has reflected upon the architecture of the internet and its qualities, but more importantly, on the interaction of individuals with the virtual world. In terms of the theoretical approach, this nexus and its criminological consequences were key to the research. At the very same time, the internet serves as a tool for the study, with the

online questionnaire being used to collect online data. The questionnaire survey was administered through many social networks, and consequently benefited from several online qualities, such as asynchronous communication, easy access, anonymity and memetism. According to Bryman (2012) and Hooley et al. (2012), online surveys (as opposed to postal surveys) have a number of the advantages (and disadvantages) (see Tables 3 and 4 respectively).

**Table 3. Advantages and disadvantages of online surveys (Bryman 2012, pp. 676-677)**

<b>Advantages</b>	<b>Disadvantages</b>
Low Cost	Low response rate
Faster Response	Restricted to online population
Attractive formats	Requires motivation
Mixed administration	Confidentiality and anonymity issues: in relation to surveys sent by e-mail
Unrestricted Compass	Multiple replies
Fewer unanswered questions	
Better response to open questions	
Better data accuracy	

**Table 4. Advantages and disadvantages of online surveys (Hooley, Marriott & Wellens; 2012, pp. 33 and 43 (citing Cantrell & Lupinacci, 2007, 2008; Fleming & Bowden, 2009; Madge et al. 2006))**

Advantages	Disadvantages
Speed and volume of data	Sample bias
Saving in costs	Measurement error
Flexible design	Non-response bias
Data accuracy	Length, response and drop out rates
Access to research populations	Technical problems
Anonymity	Ethical Issues
Respondent acceptability	

It is worth noting that the online questionnaire benefitted from many of the advantages mentioned in Table 3 and Table 4. The questionnaire itself was quick and easy to design, launch and edit with the Google Drive platform, and it proved to be an extremely effective instrument, which was important given the limitations of resources in this study. The major advantage is that the online questionnaire allowed the researcher to gather large quantities of data quite fast. Considerable effort was invested in the design of the questionnaire, trying to make it interesting, attractive, and easy to understand and complete. The careful piloting process may have been fundamental in achieving the aforementioned qualities. According to Madge, O'Connor, Wellens, Hooley, and Shaw (2006, p. 51), cited in Hooley et al. (2012), the following procedures should be followed to improve response rates:

1. Send introductory letter outlining project and estimated time needed to complete the questionnaire.
2. Include an institutional/official website to help validate researchers' identity.
3. Provide clear instructions on how to complete the questionnaire.

4. Request personal information at the start of the questionnaire rather than the end.
5. Use simple questionnaire format and avoid unnecessary graphics.
6. Avoid grid questions, open-ended questions and requests for email addresses.
7. Design the survey so that it takes approximately 10 minutes to complete.
8. Do not include more than 15 questions.
9. Send one or two follow-up reminders.
10. Include 'social presence' (information to increase trust in the researchers) or missing data messages (thanking participants for completing the survey and informing them about their progress within it) to reduce item non-response.
11. Emphasise confidentiality.

The majority of these items were taken into consideration during the data collection process, with the obvious exception of including 'less than 15 questions', as the Gramsick scale itself consisted of 24 different items.

The number of completed questionnaires submitted and the speed at which they were submitted surpassed the researcher's initial expectations. This outcome was due in part, it is believed, to the researcher's monitoring of the process. The researcher took a quite active role in the survey, which included motivating, thanking and encouraging respondents. This was done by posting several messages in Twitter, LinkedIn, Facebook and Google+, reminding potential respondents of its availability and inviting people to participate, as well as thanking those who replied and sharing messages of encouragement from other respondents.

In addition to this, and in order to guarantee further responses, the online questionnaire was administered onsite (via MOODLE) to several classes. The survey was administered to these students in their classes as it had been previously uploaded to the Virtual Campus. Students had access to the internet; they were informed viva voce by the researcher about the nature

of the research and all relevant ethical issues including consent. Students could opt-out at any moment by closing the questionnaire, but they did not have to leave the classroom. Approximately, 150 students were recruited this way. That process enabled the respondents to have direct contact with the researcher, and thereby raise and have addressed any doubts they might have. Given the process by which the online questionnaire was administered, anonymity and confidentiality were guaranteed, with replies being automatically saved on a spreadsheet stored in Google Drive.

### **3.3.4. Reliability, validity and generalizability**

#### **3.3.4.1. Reliability**

Bryman (2012) defined reliability as the “consistency of a measure or concept” (p.169). In relation to reliability, Bryman (2012) talked about “stability”, “internal reliability” and “Inter-observer consistency” (p. 168-170). Stability refers to the measure being stable over time. The self-control scale has been used in several studies, through time, and has proven to be a stable instrument (including via the PADS+ study by Wikström et al. (2013)). In regards to internal reliability or consistency, the Grasmick scale has been tested and has satisfied that criterion (Grasmick et al, 1993; Romero et al., 2003). This includes the Spanish translation as explained before. Reliability tests were conducted on the self-control scale. Cronbach’s  $\alpha$  for the aggregated self-control variable= .85, indicating very good reliability. However, if we apply the test to the different factors of self-control, Cronbach’s  $\alpha$  shows good, yet somewhat lower reliability (temper= .72, egotism= .63, physical activities= .68, risk-seeking= .72, simple tasks= .67, impulsivity= .58). This is consistent with Grasmick et al.’s (1993) indication that the ‘six components ... appear to coalesce into a single personality trait’ (p.17) and their suggestion to use the aggregated measure of self-control (p.17).



Vignettes, on the other hand, could not satisfy these criteria as they ask about independent scenarios and situations, and they do not form a 'multi-item measure' (Bryman, 2012, p.170) (unlike the Grasmick scale).

Finally, "inter-observer consistency" (Bryman, 2012, p. 169) is a factor that should not be considered, as it comes into play when more than two or more observers are coding data. In this study, most of the categories were based upon earlier studies and other theoretical approaches, yet the data was coded by the present researcher only.

#### **3.3.4.2. Validity**

As already indicated, both the original Gasmick scale and its Spanish translation (by the Universidad de Santiago de Compostela), have featured in criminological research for quite a long time.

In order to test validity (in this case face validity - see Bryman, 2012, p. 171), the online questionnaire was piloted four times by the same group of people (including criminologists, lawyers, students and people from unrelated fields). Various issues, including grammar, spelling, clarity, timing, and comprehension of vignettes and questions, were examined. All recommendations were acknowledged and the text underwent several revisions before being published. One of the major issues that arose during the piloting was the perspective from which the vignettes should be evaluated, as respondents were asked to rate actions from a moral standpoint that needed to be expressed clearly.

Vignettes were based upon easy to understand cybercrimes that implied a certain sense of familiarity, on the part of the respondent, with certain activities involving the use of new technologies or even with cybercrimes themselves. Especially technical cybercrimes (such as hacking) were ruled out, as were those involving child abuse. Respondents might have experienced illegal downloading, sexting or cyberbullying in more ways than they might have experienced child abuse (for example). This proximity might refer to respondents being actors, victims, or someone close to them being either.

The vignette technique for measuring morality has been used and tested by Schoepfer and Piquero (2006) and by Wikström et al. (2013). This study tried to draw from that research experience, using the same approach and measuring items (morality) by using the same scales, thereby profiting from already established and proven instruments.

#### **3.3.4.3. Generalizability**

The sample, as indicated before, was non-probabilistic and was derived mainly from social networks interactions (for example re-tweets and shares). On the one hand, the intention of obtaining a general view on attitudes towards cybercrime amongst internet users was partially satisfied, as the sample was comprised mostly of young university students.

All in all, obtaining a representative sample in online research it's extremely problematic as the number of people using the internet grows every day. In Spain, there were 35,010,273 internet users in 2014, whereas worldwide the number of users in 2014 reached 2,925,249,355 (Internet Live Stats, 2015). According to the International Communication Union (ITU, 2014)),

in their report *Measuring the Information Society* “by end 2014, almost 3 billion people will be using the Internet” (p. 15) and “Internet usage is growing steadily, at 6.6 per cent in 2014 – 3.3 per cent in developed countries and 8.7 per cent in developing countries” (p. 15). Therefore, a social and cultural divide existed between developing and developed countries. As the International Communication Union (ITU, 2014) has pointed out: “more than three out of four people are online in the developed countries, one out of three is online in the developing world” (p. 15). As indicated before, the majority of frequent internet users in Spain, according to official statistics (INE, 2014), are within the 16-24 and the 25-34 year age groups. However, there are no studies and statistics as to the characteristics of users of social networking sites in Spain. All in all, young people/adults dominate internet use in Spain, therefore a university sample can provide a good insight into the views of “people in general” regarding their internet use.

### **3.3.5. Analysis**

In order to analyse the quantitative strand of data, SPSS 20 (IBM, 2015) was used. The Google Drive data-sheet, with all the replies, was uploaded into the programme and the variables were then recoded. The timestamp was deleted before the upload. As indicated, the neutralisation technique replies were coded into dummy variables.<sup>15</sup>

After the coding process, a total number of 126 variables had been created. These covered participant socio-demographics, Grasmick scale items, morality and engagement variables, and neutralisation variables. Other variables were then computed (for example, the aggregated

---

<sup>15</sup> Dichotomous categorical variables that only contained values 0 and 1. 0 indicated that the respondent did not pick that specific technique in that specific scenario, whereas 1 indicated the respondent had picked that technique in that scenario.

self-control measure). Several statistical tests were performed to find patterns and relationships between different variables, following what was theorised about the SAT-RI. The tests performed were T-Tests, ANOVA, chi square tests and regressions for statistical hypothesis testing.

### **3.4. Interviews with Law Enforcement Agents**

#### **3.4.1. Sample**

While a general idea on the “baseline morality” relating to the Internet was being collected via the questionnaire survey, a series of interviews took place in order to obtain information on cybercriminals’ thoughts. As discussed previously, contacting cybercriminals raised major ethical and access issues that could have hindered the adequate and timely development of this research.

As a result, a decision was taken to use police officers as “proxies” in order to understand the motivations and neutralisations behind the actions of cybercriminals. In Spain, two national police corps co-exist (Guardia Civil and Spanish National Police) both of them with specialised cybercrime Units. After solving major access issues, five interviews took place: one Guardia Civil, three National Police Officers and one former National Police officer now working for the private sector. The intention was to obtain different perspectives and approaches to cybercrime and the thought process of the cybercriminal, also a more varied catalogue of crime cases.

In terms of sampling procedure, this was a non-probabilistic, convenience sample, as only those volunteering were interviewed. Considering that Cybercrime Units are highly specialised police corps, comprised of a small number of members, the population from where the sample stems is very small.

After negotiating access with the respective law enforcement agencies, the sample ended up being limited to those volunteering to take part, and those officials who had sufficient knowledge of cybercrime and professional experience in the field. The fact the study comprised five interviews is not a matter of major concern as the case study approach (three or more cybercrime cases discussed per person) resulted in the generation a sample of a 20 cybercrime cases. Finally, a gatekeeper from the National Police was approached and the researcher gained access to three Unit Chief Inspectors (From the Open Networks Division, the Logic Defence Division and the Child Protection Division) from Policía Nacional. Interviewees and their professional roles are coded as indicated Table 5.

**Table 5: List of pseudonyms for law enforcement agents**

<b>Expert List</b>	<b>Affiliation</b>	<b>Professional Experience</b>
<b>GCEX</b>	Guardia Civil (GDT)	17 years
<b>PSEX</b>	Private Company (Former National Police)	13 years National Police + 5 years Private Sector
<b>NPEX1</b>	National Police (Open Networks)	4 years
<b>NPEX2</b>	National Police (Logic Defence)	5 years
<b>NPEX3</b>	National Police (Child Protection)	14 years

Table 5 is a good indicator of the expertise amassed by the experience in the fields of cybercrime. Interviewees had varied length of experience and quite diverse positions currently, therefore having different perspectives in terms of investigation cybercrime. The experience described does not refer to their general police experience, but to their experience in the cybercrime field. NPEX 1 is in charge of the Open Networks Division<sup>16</sup> of the National Police, NPEX2 is in charge of the Logic Defence Division<sup>17</sup> of the National Police, whereas NPEX3 is in charge of the Child Protection Division, all of them within the Cybercrime Unit. GCEX, on the other hand, is a sergeant at the Guardia Civil<sup>18</sup> working for the Guardia Civil

---

<sup>16</sup> This Division investigates crimes committed in social networks and crimes that are not investigated by the other Cybercrime Divisions of the National Police (for example, cyberfrauds).

<sup>17</sup> This Division investigates the commission of hacking offences or the creation and dissemination of virus or malware.

<sup>18</sup> In Spain, the Guardia Civil has a militarized structure therefore agents hold military ranks. Contrarily, The National Police is a purely civilian public institution.

Cybercrime Unit. PSEX is currently working as a security consultant, for a private firm, but he/she has several years of experience as a police officer in the cybercrime field.

Once the coding took place a list of 20 cases was produced. The qualitative analysis sample is based on these case studies, it can be indicated that the sample is big enough and diverse to work with, cases represented a variety of crimes such as scams and frauds, hacking, malware offences, child sex pornography, child grooming and sextortion and industrial espionage. According to the Internet Crime Complaint Centre's 2014 Internet Crime Report, frequently reported crimes were essentially scams and frauds like "Auto Fraud" (a cyber Fraud involving the scam sale of a car) (IC3, 2014, p. 10), Government Impersonation E-mail Scam (a form a phishing) (p. 11), Intimidation and Extortion (p. 12), Real State Fraud (p. 13) and Romance Scam (p. 14). Official statistics on other type of cybercrimes are very difficult to find, given the dark figure of crime that likely applies to such a complex criminal phenomenon. The Cybercrime Unit from the Guardia Civil publishes tips and news on recent and new forms of cyber-crime in order to raise public awareness, as an example: "Holiday apartment rent scam" (GDT, 2015), "The Police Porn Virus" (GDT, 2014) or "*Cryptolocker*" (GDT, 2013). CEOP recognizes that the key threat children face in the UK are "the proliferation of indecent images of children" (2013b, pp. 8-9), "online child sexual exploitation" (pp. 10-13), "transnational child sexual abuse" (pp. 14-17) and "contact child sexual abuse" (pp. 18-21).

However, two cases were ruled out from the matrix, because they did not satisfy the theoretical criterion established in the theoretical framework in order to be considered cybercrimes. Invalid cases were C5 "The Solitaire" and C6 "The Kid with the katana", narrated by PSEX. C5 talked about the entrepreneur of a well-known thief that, according to the interviewee, used the computer in order to plan escape routes or disguises. C6 was another

relevant Spanish case about a minor with psychological problems who killed his family with a katana (allegedly inspired by The Final Fantasy videogame). The reason PSEX considered it a cybercrime was owing to the offender writing a letter on a computer explaining his situation. In both cases, the use of computers is extremely incidental and not instrumental. There was not a profound rapport between the offence and the internet (or the machine), and consequently no relationship with the variables examined in the present study. Finally, C12 “Nitro”, identified by NPEX1 is only partially valid as it presents a very interesting case in relation to vanity, ego, social networks and crime (from the point of view of the offender), but the case, about illegal races uploaded onto Youtube, was judged, by the present author, not to satisfy the cybercrime criterion. The final sample analyses for this part of the research comprised 17.5 cases. Case categories were “Child Abuse and Pornography” (referring to Cases C2, C4, C18 and C19), “Cyber Fraud” (C3, C8, C10 and C11), “Hacking” (C1, C7, C9, C16 and C17), “Child Grooming” (C20), “Hacktivism” (C15), “Malware” (C13 and C14) and “Unclassified” (C12).

It is worth mentioning that the cases were extremely heterogeneous and they talked about the major types of cybercrime. Furthermore, some of the cases (for example Anonymous, Police Porn Virus and Siglo XXI) are extremely recent, therefore investigations are fresh and the interviewees were professionally involved in them. Also, the “*Nannysex*” Case (C4 by PSEX and C18 by NPEX3) was discussed by two interviewees. However, and given the relevance of the case and impact on Spanish culture, both reports were used. Finally, when prompted by the researcher PSEX talked about his/her general views on cybercrime and society after the case analysis had ended. That led to what the present researcher felt were extremely interesting perceptions, which were coded as “no case”.



### **3.4.2. Instrument**

The interviews that were conducted with law enforcement agents served as good examples of research about the internet conducted using offline techniques. The researcher wanted to have direct contact with the interviewees in order to encourage them to have more trust in him, as a result of which they would provide more information and more accurate information. As mentioned in previous paragraphs, the interviews took place in the Universidad Europea de Madrid and the Spanish National Police Headquarters. Interviewees were asked about the types of crime they investigated, and were allowed to offer as much technical and procedural information as they wanted. However, they tried to use an accessible language, colloquial in some aspects and not extremely academic. Some of them also commented on certain features of the internet that have changed social patterns, values or even the very concept of family or romantic relationships.

Interviews were semi-structured and were undertaken as “case studies”. The aim was to obtain a variety of cybercrimes investigated by the law enforcement agents, the researcher asked interviewees to elaborate on three (or more) cases they had investigated explaining the investigation procedure, the results of the investigation and all possible information about the offender.

The initial procedure was the same for all interviewees. Before the sessions took place, interviewees received an e-mail with the information and consent forms (with the latter having to be signed), and a list of the topics to be discussed. The questions put to interviewees covered four major areas and were as follows:

- Experience in the field of cybercrime
- Crime: What happened? What crime was committed, how was it investigated and what was the outcome?
- Offender: Who was the offender? What did he/she do, how did he/she perceived his/her actions? How did he/she justify what he/she did?
- Special Circumstances: Were minors involved? Was there and international component? What were the social and media repercussions of the case?

### **3.4.3. Procedure**

Interviews took place on 6/06/2014, 16/06/2014, 12/09/2014 and 4/12/2014; two of them took place at the Universidad Europea de Madrid Campus, Villaviciosa de Odón (Madrid), and the rest at the National Police Headquarters in Madrid. All interviews were voice recorded and notes were also taken in order to facilitate coding. All interviews were transcribed and all transcriptions were stored safely under a password protected platform and on several hard-drives. After all the interviews were transcribed and uploaded into the NVivo software, original audio files were deleted. For the transcription procedure, a research assistant was recruited to the project.

Just before the interview commenced, the researcher reminded participants of the matters covered by the information and consent forms, and obtained written consent from them, once the interview commenced the interviewer explained again the information and obtained verbal consent that was recorded. After that, interviewees were reminded of the overall structure of the interview and were given three cards with all the questions as visual aids in order to help them organise their thoughts.

During the interviews, the researcher explained to participants that although they were being asked about specific cases and to a set structure, this was not rigid and interviewees were welcome to add whatever information they desired. Also, different questions were added by the researcher through the interviews as prompts or probes, whilst allowing the interviewee to navigate the information as they preferred.

In relation to translations, Spanish transcriptions were imported into NVivo and were coded in English. Relevant passages have been translated into English by the researcher in order to be used as in-text resources. The researcher has comprehensive experience in working with English and Spanish texts, simultaneously, in the fields of social sciences, more specially law and criminology. This follows on from his experience both as criminology and a law lecturer, and a legal practitioner in Spain and in the UK.

#### **3.4.4. Reliability, validity and generalizability**

According to Bryman (2012, pp. 390-394, citing Lincoln and Guba (1985) and Guba and Lincoln (1994)), qualitative research can be evaluated according to different criteria, such as: trustworthiness (comprising credibility, transferability, dependability and confirmability) and authenticity. Yardley (2000), cited in Bryman (2012, p.393-394) mentions the criteria of sensitivity to context, commitment and rigour, transparency and coherence, impact and importance. These are the qualities that the researcher endeavoured to follow in the present study.

Interviewees were asked about their experience in the field. All of them had the necessary education, training and experience to offer relevant and critical approaches to cybercrime. Moreover, all of them had experience in dealing with offenders at some point in their careers and some of them were in charge of different operational groups. The experience of police officers served as an indication of the rigour of their narrative, but also of their commitment to law enforcement and their trustworthiness. In many of the criminal cases that were discussed, the interviewees shared materials - such as photographs, videos , court reports, investigative diagrams, webpages and features from different newspapers - with the researcher (NPEX1, NPEX2, and NPEX3 used these materials in all of the cases they discussed).

In addition, even though all the cases discussed contained sensitive and confidential information, law enforcement agents tried to back up their discourse up with media sources (for example material from TV, You Tube and newspapers), legal documents, and photographic

and forensic evidence, thus helping to triangulate their data (Bryman, 2012, p 392; Silverman, 2010, p. 277). It is worth remembering that although the sample could be viewed as small, in terms of the number of interviewees, the data was collected on “a case study basis”.

Each interviewee was asked about three different cybercrime cases he/she had been involved in (some of the interviewees talked about more cases). In other words, interviewees constituted part of the sample (the source of data), and the cases they discussed the part used for testing the theory. That is the reason why interviewees were asked to provide varied cases - if possible - in order to obtain a broader picture of the investigation of cybercrime.

It is also worth mentioning that the researcher tried to obtain the most unadulterated form of data from the interviewees, including factual information and personal opinion, letting interviewees talk as much as they wanted, and allowing them to add or address any related issues. In order to achieve this, the idea of semi-structured interviewing was emphasised to participants, so that they considered certain specific topics but also had the opportunity for wider discussion. In the case of PSEX, for example, the case study was explained quite quickly, so the researcher asked follow-up questions, before the interview ended, in order to obtain more information. This led PSEX to discuss certain social issues and social changes fostered by the ubiquity of digital technologies. This final part of PSEX's interview did not relate to any particular case and was labelled “PSEX's diatribe”.

A critical approach was taken in terms of analysing the data to understand what approaches derived from a police culture, and which are either professional or personal opinions. Police culture can be extremely binary in terms of its conception of morality (for example, the idea of

‘good’ versus ‘evil’ or ‘US’ against ‘THEM’, which can stem from their constructed ideology (Reiner, 2010). However, individuals from the sample demonstrated social sensitivity and a profound empathic capacity in relation to the understanding of criminal aetiology and context, possibly developed through years of field and investigation work, and from their education in law, criminology, psychology or science.

### **3.4.5. Analysis**

For the analysis of the qualitative strand of data, NVivo 10 (QSR International, 2015) was used. All of the transcriptions were uploaded into the programme for coding (a summary of all the cases and relevant information about them is contained in Annex X).

For the main analysis the information was coded following Grounded Theory (Gibbs, 2010a, 2010b, 2010c, 2010d, 2010e, 2010f, 2010g, 2010h). As subsidiary analysis, a narrative discourse analysis of the police discourse data was also carried out (following Foucauldian approaches (Gibbs, 2015)) and along with narrative analysis (following Esin, Fathi, & Squire’s (2014) constructionist approach). Police culture was analysed, and the researcher tried to understand how it affected the interview data, and the law enforcers’ personal creation of the cybercriminal and their understanding of criminal motivations. The narrative analysis and the ideology of police culture (Reiner, 2010), mentioned here will be explained in more detail in the qualitative analysis chapter. After the analysis, two essential categories emerged: offender morality and neutralisation techniques. No discourse on self-control was found (as expected) in the case studies. At the same time, new codes, which were not contemplated or predicted in the theoretical framework, emerged and were later considered for the qualitative analysis and the integrated analysis.

Finally, during the analysis, care was taken in analyzing the meaning of language. That is the reason why during the translation phase, the current researcher tried to respect the essence of the original Spanish texts regarding slang words and the personality of the interviewees. The researcher saw this as an essential task, in order to disentangle the possible cultural bias and to discuss the reliability of the accounts. All of the translations used in this work (from Spanish into English) were done by the researcher.

A core issue relating to the analysis was the use of second-handed testimonials. McMyler discusses the epistemological issues that the idea of “knowing at second hand” (2007) can rise. Firstly, “an item of knowledge is testimonial if and only if it is secondhand in the demanding sense of being justified by the authority of the speaker” (p. 520), the idea of “authority” becomes therefore central to his discussion on how can we perceive reality through others, yet said authority can be accepted or challenged at some point:

The epistemic authority with which a knower thinks and speaks about her knowledge gained from a particular epistemic source has to do with the kind of justification appropriate to knowledge based on the source” (McMyler, 2007, p. 523) ... an epistemic authority that entitles the audience to defer challenges to its testimonial knowledge back to the original speaker (McMyler, 2007, p. 527)

At the same time, audiences are to be cautious and judgmental in relation to the authority of the speaker and the testimonial (that becoming a responsibility of sorts) but not being entirely untrustworthy (p. 534). In terms of authoritative knowledge, higher ranking law enforcement agents with plenty of experience in the fields they are speaking about, and having in addition a good level of education in the fields of crime control, are worthy of trust (Ministerio del Interior [Ministry of Interior], 2006). On the other hand, their extensive experience might have cemented certain views, in their minds, through time and an institutionalization may have

taken place in which a caricature of the criminal is formulated. In order to identify and address those issues, narrative analysis was employed in analysing the data.

In relation to the narratives underlying the interviews, a constructionist approach to narrative analysis takes into consideration not only “the linguistic minutiae of the construction of a story between speaker and listener” (Esin et al., 2013, p. 203), but also broader social issues. The audience becomes extremely important, but power relationships and context also play a fundamental role (p. 205-206). Power relationships are transmitted in the way the cybercriminal is constructed as according to law enforcement agents, in terms of how interviewees value and rate the morality of offenders or explain their role as agents of a benign social order. Other relevant issues in terms of narratives are those relating to translation (Esin et al., 2013, p. 208).

A similar approach to narrative analysis is “Critical Discourse Analysis”, orientated towards the understanding and critique of social issues inherent in discourse (Gibbs, 2015; Lê & Lê, 2009). Social change, inequality or the abuse of social control are important social issues that relate to crime and law enforcement, and which should be discussed when analysing the interviewees’ discourse, along linguistics, power and the construction of meaning (Lê & Lê, 2009) and ideology as presuppositions, cliché or implicature (Lê & Lê, 2009, p. 12). In this thesis a Narrative/Discourse Analysis was adopted but this did not incorporate in-depth critical discourse analysis. This is due to the fact that policing is not the focus of the thesis. The main issues that were addressed were language (essentially translation), ideology (as police culture) and power relationships embedded in the discourse.



Finally, second-hand police narratives, acting as “proxies” offenders’ accounts, are inherently subjective as any narratives or discourses would be, a ragbag of visions can be found. This is because these narratives involved, first, the police officer’s view (personal or professional); secondly, the offender’s view; and thirdly, the academic or theoretical view assumed by the police as an institution. Ideally, these three distinct perspectives should be separated from one another in the course of the narrative analysis.

### **3.5. Ethics**

The study gained ethical approval from the School Research Ethics Panel (School of Human and Health Sciences, University of Huddersfield). The main ethical issues to be considered were:

- Safety and Risk: The study posed no significant risk, either to the researcher or the respondents. The questionnaire was launched online for respondents to answer at their own discretion. Thus, the researcher did not need to travel in order to collect data. In relation to “captive” audiences (the use of students during classes), the data collection procedure took place during lectures and in lecture rooms at the Villaviciosa Campus of the Universidad Europea de Madrid. In addition, interviews with law enforcement agents took place at the aforementioned campus and at the Spanish National Police Headquarters. Both of these venues were considered safe environments.
- Information and consent: Participants were informed of the aims of the study by using appropriately modified versions of the University of Huddersfield information and consent sheet templates. For the questionnaire, this information was uploaded online

and appeared in the first page of the questionnaire. Respondents were asked to tick all relevant boxes if they wanted to proceed to the main body of the questionnaire. Students were also informed in person, during classes and by the researcher of: the purpose of the study, anonymity, confidentiality and the voluntary nature of the study. If students wished to ask questions during the survey these were addressed and resolved by the researcher.

For law enforcement agents, copies of the documents (consent and information forms) were sent by e-mail, and the copies for the researcher were collected before the interviews took place. Interviewees also kept a copy of their signed documents. Verbal information was given about the purposes of the study and relevant ethical issues such as anonymity and confidentiality even though the interviewee was already informed via the consent forms. Consent was, therefore, obtained in written and spoken form.

-Anonymity and confidentiality: The Google Drive web-based questionnaire facility stores all submitted information in a data-sheet, making it impossible to determine the identity of the respondent. This information was subsequently analysed in SPSS as aggregated data.

Interviews were recorded and transcribed with pseudonyms were used in place of interviewees names. The research assistant in charge of transcriptions signed a “non-disclosure” contract and he did not have access to any personal information relating to interviewees. After the transcriptions were made, the audio recordings were deleted.

Data was securely stored under password-protected “cloud” storage as well as in three different hard-drives. Hard copies are safely guarded by the researcher.

- Harm and Distress: Respondents were not asked to reveal sensitive or distressing information during the data collection process. All questions could be left unanswered should the respondent have desired to do so. Interviewees were asked questions relating to their jobs and daily experiences (law enforcement). They were allowed to elaborate as much as they desired on the topics at hand. The researcher tried to create a relaxed and confidential atmosphere, given the delicate nature of some of the information dealt with.

### **3.5.1. Ethics in an online environment**

Online research presents particular ethical issues and some of these had to be addressed in the course of this research. Some of these have been covered in previous sections of this chapter. According to Hooley et al. (2012, pp. 25-38), the main ethical issues in online research are: privacy, informed consent, anonymity and confidentiality, legal issues and participant vulnerability.

In relation to privacy, Hooley et al. (2012) explain the existence of:

a blurring of the boundary between what is public and private data on the web, and puts researchers in a difficult position where they have to consider whether users' perceptions of their own privacy align with the "public" nature of the interface they are utilizing. (p. 31)

In this case of the present study, the data obtained from the survey was not collected from public forums (like messages boards or social networks), but was provided willingly by respondents by means of the anonymous online questionnaire, accessible only if the link

provided by the researcher was clicked. On the other hand, some of the law enforcement agents used videos found in YouTube (for example NPEX1), which had been subject to police investigations, to illustrate the points that were being presented by him/her. In these situations, the videos remained between the researcher and the interviewee, and did not feature as ancillary data (despite the fact that they are public). Other interviewees like NPEX3 and NPEX2, used webpages during the interviews to illustrate their points (for example, pages where hackers boasted of their deeds) their comments on that pages and recoded but no webpages an annexed.

In relation to informed consent, Hooley et al. (2012) indicated that “the online nature of the interaction between the researcher and potential participant, especially if text-based and asynchronous, can make it more difficult to ensure that the participant has sufficient information” (pp-33-34). That is the reason why a not inconsiderable amount of effort was invested in ensuring that the informed consent obtained in relation to the online survey, was valid. Clear and comprehensive Information about the survey was presented before the online questionnaire commenced and participants were invited to tick various boxes to ensure that they had been adequately informed and that they consented to all the conditions of the research. When questionnaires were administered in classes, this information was provided verbally, by the researcher, to the students before they commenced the survey. Anonymity and confidentiality have been discussed in this chapter in detail.

Finally, no legal issues arose as no personal data was obtained from personal sites (like social networks or communities) and no illegal sites were consulted. And in relation to participant vulnerability, no sensitive groups were approached and no sensitive online data was accessed.

It has to be borne in mind, once again, that the questionnaire was designed as indirect questioning in order to avoid self-reporting crimes from participants.

## **Chapter 4: Findings - Online Survey on Attitudes Towards Cybercrime**

### **4.1. Demographics**

The sample was 43.4 % (N=308) male and 56.6 % female (N=401). This does not seem to represent any major imbalance, gender-wise, in the sample. This gender mix was probably a reflection, in part, of the gender bias amongst University students and also the general population in Spain.

According to INE (2005b), in 2010-2011, of the 905,229 students enrolled in higher education, 483,203 (53.38 %) were women. Similarly, the population in Spain, in 2014, comprised 51.31% females and 48.69 % males. Therefore, a higher number of female respondents to the survey could have been expected.

The gender variable can offer an interesting insight into how crime may be perceived differently by women and by men, and how their levels of self-control might vary. This is analysed later in this chapter.

The mean age of the sample (N= 706) was 28.36 (SD= 10.02) and the mode 23 years. It is evident, then, that the sample was comprised largely of young adults. Interestingly, although the majority of participants fall within the category of university students, 28 and 23 years do not fall within the usual age frame for university students in Spain. Degrees are 4 years long and students usually enter university at 18, usually finishing at 21/22. However, this is just the

typical case and it is not mandated. In addition, the sample may have contained (older) Masters and Doctoral students, as these groups were also invited to take part in the survey. In terms of outliers, the ages of 16 and 17 or 60, 64, 67, 69 appeared in the sample. Older generations are, therefore, underrepresented in the sample, as are adolescents.

In terms of occupation (N=709), the majority of the survey sample comprised "University Students" (56.8 %). Relatively small proportions of respondents were drawn from a variety of other occupational groups. These were as follows: "Education, Research and Languages" (7.9%), "Public and Private Security Corps and Military" (6.9 %), "Legal" (6.1%), "Unemployed" (4.1%), "Clerical and Administration" (3.8%), "Information, Communication and Finance" (3.7%), and "Health and Wellbeing" (3.4%). The rest of the occupations were not deemed to be representative as numbers were very small: "Other" (7.3%), yet it must be taken into consideration that 16 occupations were coded in total, following international normalised standards of occupations (ILO, 2004), as explained in Chapter 3. This over-representation of university students is easily explained when account is taken of the fact that the researcher is a lecturer, and part of the data collection process took place at Universidad Europea de Madrid, during classes. In addition, the questionnaire was posted on Twitter, Facebook, LinkedIn and Google+.

In terms of nationality (N=709), 91.1 % of the participants were Spanish. The remaining 8.9 % were mostly from Spanish speaking countries (like Mexico, Peru and, Venezuela) and a very small number European from countries (like Portugal, Holland, Switzerland, France, and Italy). This variable was, therefore, left out of the analysis, because of the vast majority of the sample being Spanish.

Over two-thirds (68.7%) of the sample (N=709) reported that they had been the victim of a crime in the last year, with 31.2% stating that they had not. One respondent chose “yes” and “no” in answering this question, and so this individual has been left out of the study. As this thesis is focused upon perceptions of morality of criminal behaviour, it was felt to be particularly important to examine the influence of criminal victimisation and in particular the ratings of crime as morally noxious. A chi-square test was performed and showed no significant statistical difference between males and females with regards to whether they had been a victim of crime or not  $\chi^2(1, N = 708) = 0.40, p > 0.05$ .

Therefore it can be assumed that being a victim of crime is not distributed according to gender within the sample.

## **4.2. Self-Control Scale**

The self-control scale was based upon Grasmick et al. (1993), who tried to measure self-control drawing on Gottfredson and Hirschi's (1990) work *A General Theory of Crime*. The scale is comprised of 24 items that can be grouped into the six theorised elements of self-control.



Grasmick et al. suggested that the scale should be used to measure a composite trait (self-control):

A single, unidimensional personality trait is expected to predict involvement in all varieties of crime, as well as academic performance, labor force outcomes, success in marriage, various 'imprudent' behaviors such as smoking and drinking and even the likelihood of being involved in accidents. (p. 9)

After empirically studying the six elements of self-control, using their own scale, Grasmick et al. arrived to the following conclusion:

Instead, from an empirical perspective, the strongest case can be made for a one-factor unidimensional model .... Our conclusion is that the six components we have identified as Gottfredson and Hirschi's definition of low self-control appear to coalesce into a single personality trait. (p. 17)

However, in this thesis, when analysing the data, in order to find an overall pattern of self-control, the six elements of self-control were treated separately in terms of descriptive statistics and compared to the engagement and morality variables. Finally, high levels of self-control were found in the sample and the decision was made to use only the aggregated "coalescent" self-control variable in the present study.

The self-control variable therefore played an important role in this study. It is important to make clear that the scale used in this study is not the original one from the Grasmick study, but a translation into Spanish by Romero et al. (2003). It differs from the Grasmick et al.'s scale only in the order of the questions. Despite this difference, the Romero et al. /Spanish scale

Cronbach's  $\alpha$  for the 24 item matrix = .85 indicating very good reliability (as mentioned in the methodology chapter). In addition, correlations were tested between all 24 items in the scale, indicating very significant correlations. The majority of variables correlated positively.

The values for the answers were: 1= Strongly disagree; 2= Disagree somewhat; 3= Agree somewhat; and 4=Strongly agree. It must be borne in mind that low scores indicate high self-control.

The highest rated item (GrasmickItem3: "I like to test myself every now and then by doing something a little risky") had a mean of 2.63 and a Mode of 3, being the question that leans most towards low self-control. No other item had a mean higher than 3 or a mode equal to 4. The lowest mean (1.59) can be found in GrasmickItem23 ("I will try to get the things I want even when I know it's causing problems for other people"). In addition, 14 items had a mean lower than 2; whereas 10 items had a mean higher than 2 but lower than 3. At first sight, this seems to indicate that the sample had high levels of self-control (scores less than 3 range). As indicated in the theoretical framework, high levels of self-control (following Gottfredson & Hirschi, 1990), would mean that the sample is able to postpone pleasure and deal with frustration, therefore not likely to engage in acts of crime.

Once the self-control items had been measured, items were grouped into six different elements - as theorised by Grasmick et al. (1993), following on from the work of Gottfredson & Hirschi (1990). These elements of self-control and the grouping of items can be seen in Table 6.

**Table 6. Descriptive statistics of the Grasmick scale items**

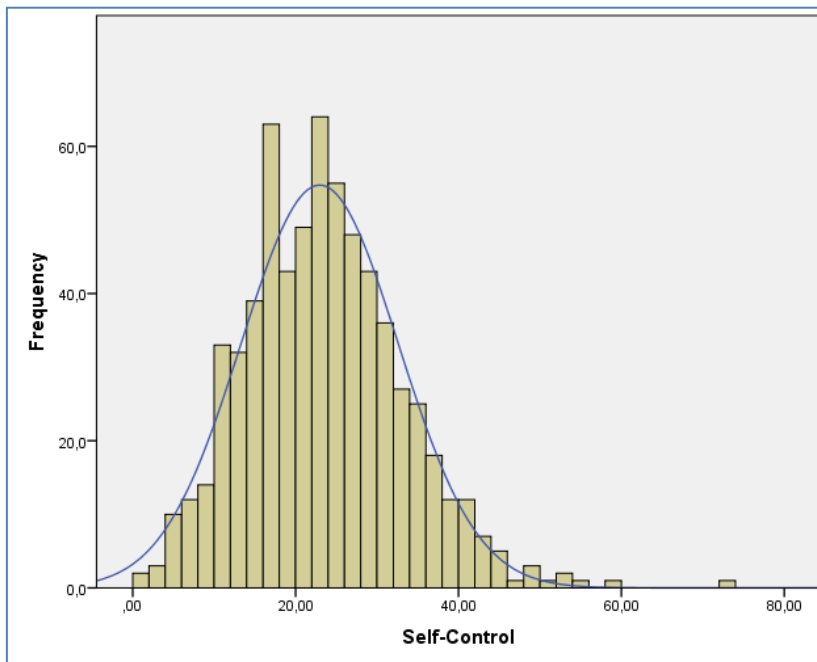
	Content of element	Descriptive statistics
<b>Impulsivity</b>	GrasmickItem1 ( "I often act on the spur of the moment without stopping to think") GrasmickItem7 ( "I don't devote much thought or effort to preparing for the future") GrasmickItem13 ( "I often do whatever brings me pleasure here and now, even at the cost of some distant goal") GrasmickItem19 ( "I'm more concerned to what happens to me in the short sun than in the long run")	GrasmickItem1: M= 2.13; Mode= 2; S.D.= .88 GrasmickItem7: M=1.74; Mode=1; S.D.= .85 GrasmickItem13: M= 1.73; Mode=1; S.D.= .83 GrasmickItem19: M=2.16; Mode=2; S.D.= .88  <b>Impulsivity: M=4.77; Mode=5.00; S.D.=2.28</b>
<b>Simple Tasks</b>	GrasmickItem2 ( "I frequently try to avoid projects that I know will be difficult") GrasmickItem8 ( "When things get complicated I tend to quit or withdraw") GrasmickItem20 ( "The things in life that are easiest to do bring me the most pleasure") GrasmickItem14 ( "I dislike really hard tasks that stretch my abilities to the limit")	GrasmickItem2: M= 1.79; Mode=1; S.D.= .82 GrasmickItem8: M=1.68; Mode=1; S.D.= .79 GrasmickItem20: M=2.01; Mode=2; S.D.=.84 GrasmickItem14: M= 1.77; Mode= 1; S.D.= .78  <b>Simple Tasks: M=4.25; Mode=4.00; S.D.=2.23</b>
<b>Risk Seek</b>	GrasmickItem3 ( "I like to test myself every now and then by doing something a little risky") GrasmickItem9 ( "Sometimes I will take a risk just for the fun of it") GrasmickItem21 ( "I sometimes find it exciting to do things for which I might get in trouble") GrasmickItem15 ( "Excitement and adventure are more important to me than security")	GrasmickItem3: M= 2.63; Mode=3; S.D.= .86 GrasmickItem9: M= 1.79; Mode=1; S.D.= .87 GrasmickItem21: M= 1.68; Mode= 1; S.D.= .82 GrasmickItem15: M= 1.75; Mode=1; S.D.= .79  <b>Risk-Seek: M=4.85; Mode=4.00; S.D.=2.46</b>
<b>Physical Activities</b>	GrasmickItem4 ( "If I had a choice, I would almost rather do something physical than something mental") GrasmickItem10 ( "I almost always feel better when I am on the move than when I am sitting or thinking") GrasmickItem16 ( "I like to get out and do things more than I like to read or contemplate ideas") GrasmickItem22 ( "I seem to have a greater energy and a greater need for activity than most other people my age")	GrasmickItem4: M= 2.05; Mode= 2; S.D.= .87 GrasmickItem10: M=2.24; Mode=2; S.D.= .89 GrasmickItem16: M= 2.31; Mode=2; S.D.= .90 GrasmickItem22: M= 1.78; Mode= 1; S.D.= .92  <b>Physical Activities: M=5.37; Mode=5.00; S.D.=2.55</b>
<b>Egotism</b>	GrasmickItem5 ( "I try to look out for myself, even if it means making things difficult for other people") GrasmickItem11 ( "I'm not very sympathetic to other people when they are having problems") GrasmickItem17 ( "If things I do upset other people, it's their problem not mine") GrasmickItem23 ( "I will try to get the things I want even when I know it's causing problems for other people")	GrasmickItem5: M= 2.08; Mode=2; S.D.= .92 GrasmickItem11: M= 1.47 ; Mode= 1; S.D.= .77 GrasmickItem17: M= 1.83; Mode=1; S.D.= .86 GrasmickItem23: M=1.59; Mode= 1; S.D.= .72  <b>Egotism: M=3.97; Mode=2.00; S.D.=2.25</b>
<b>Temper</b>	GrasmickItem6 ( "I lose my temper pretty easily") GrasmickItem12 ( "Often, when I am angry at people, I feel more like hurting them than talking to them about why I am angry") GrasmickItem18 ( "When I'm really angry, other people better stay away from me") GrasmickItem24 ( "When I'm in serious disagreement with someone, it's usually hard for me to talk calmly about it without getting upset.")	GrasmickItem6: M=1.80; Mode=1; S.D.= .86 GrasmickItem12: M= 1.62; Mode=1; S.D.= .83 GrasmickItem18: M=2.36; Mode=2; S.D.= 1.00 GrasmickItem24: M=2.05; Mode=2; S.D.= .91  <b>Temper: M=4.82; Mode=4.00; S.D.=2.65</b>

These new resulting variables ranged from 1 to 13 in terms of scores with, again, low scores indicating high self-control. It is worth mentioning how the mean for egotism equalled 3.97, with such a low score seeming to indicate that the sample had a very low tendency for self-centeredness. On the other hand, the trait relating to the preference for physical activities showed the highest score ( $M = 5.36$ ). The results of several T-Tests are explained, below, comparing the means between the vignette results (variables of engagement and morality) and each of the abovementioned six elements of self-control.

In addition, all the other results (the rest of the self-control elements: impulsivity, simple tasks, risk seek, and temper) expressed a somewhat normal distribution and pointed to a sample with high levels of self-control, who were able to postpone immediate satisfaction and cope with frustration.

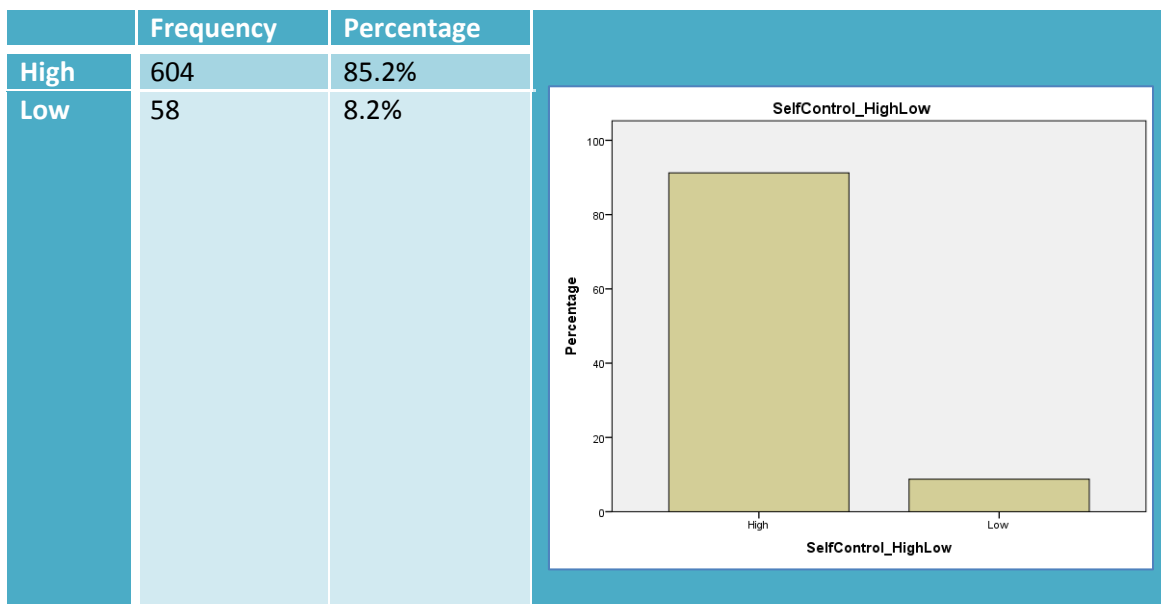
All these different elements of self-control were aggregated into a new variable called self-control, as suggested by Grasmick et al. (computed by summing the variables impulsivity, simple tasks, physical activity, risk-seek, egotism, and temper). This allowed the current researcher to understand the overall levels of self-control in the sample and relate them to other variables, such as propensity or neutralisations. The resulting variable ( $N=662$ ) ranged from 1 to 73 (Self-control:  $M=22.95$ ;  $Mode=17.00$ ;  $S.D. =9.65$ ). It must be mentioned once again that the sample demonstrated generally high levels of self-control ( $M=23$ , and  $mode=17$ ). Also, self-control leaned towards a normal distribution, albeit somehow leptokurtic as shown in Figure 8. It is also worth mentioning that was “outlier” occurred, with one respondent scoring 73, this being the lowest measure of self-control within the sample.

**Figure 8. Distribution of self-control**



In order to work in a dichotomous manner with the self-control results, facilitate groupings in comparisons and use them for the completion of *chi-square* tests and T-Tests from another perspective (by grouping respondents in groups of high or low self-control), a categorical value was computed. The new variable was called SelfControl\_HighLow. This new variable classified as high self-control results ranging from 1 to 36 from the original interval self-control variable, and as low self-control results ranging from 37 to 73 from the original interval self-control variable. A score of 36 was used as the threshold for two reasons. First, it represented the “half” of the frequencies of the original interval variable and secondly because it marked the general decrease in the frequencies (the highest densities can be found in the 30-31 scores). It must be borne in mind that it does not equal the median or the mean.

**Table 7. Frequency table and graph for the SelfControl\_HighLow variable**



As it can be seen in Table 7, high self-control was found in 85.2 % of the sample, whereas low self-control occurred in 8.2% of the sample. This is consistent with the idea of a sample with high levels of self-control.

In order to understand how self-control was distributed amongst the sample, several chi-square tests and T-Tests were performed. The first Cross Tabulation compared Self-control between gender, in order to find significant differences in the distribution of the two levels of self-control between males and females. According to the test, 86.6 % of males scored high in self-control, whereas 13.4 % of males scored low. In contrast, 94.7 % of women scored high in self-control, as opposed to 5.3 % who scored low. This indicates that women show higher scores of high self-control and lower scores of low self-control than men. A chi-square test was performed and it revealed a significant statistical difference between males and females with regards to high or low self-control  $\chi^2(1, N = 662) = 13.46, p < 0.001$ .

It is evident, then, that high self-control was distributed differentially according to gender within the sample. Also, a T-Test, which compared the aggregated self-control variable means, depending on gender, demonstrated that females had higher levels of self-control (as their means were lower)  $t(660) = 2.79, p < 0.01$ .

A further *chi-square* test showed no significant statistical difference ( $\chi^2(1, N = 612) = 0.04, p > 0.05$ ) between individuals' levels of self-control (high or low) and whether they had been a victim or crime (or not). For example, 91.5 % of the individuals who had been victims of crime, ranked high in self-control. However, 91.1 % of the individuals who had not been a victim of crime also ranked high in self-control. In addition, a T-Test using the variable victim of crime as the grouping variable, showed no significant differences between the means of both self-control samples ( $t(659) = 0.62, p > 0.05$ ).

In conclusion, women seem to have higher levels of self-control than men, but there are no significant differences, in levels of self-control, by victimisation status.

### **4.3. Vignettes**

Vignettes served to measure propensity (for the commission of cybercrimes) in the proposed SAT-RI . Two variables were taken into account: engagement and morality. Engagement was assessed through the question "Would you do it?" and morality was assessed through the question "How morally wrong do you think this is?"- The third question referred to

neutralisation techniques and this will be discussed later. The vignettes that were presented to participants can be seen, in full, in Annex 2.

Taking into account that the SAT-RI is based on the morality of the individual and his/her interaction with the morality of any given environment, it was very important to consider whether the individual might engage in cybercrimes eventually, and his/her perception of morality and immorality regarding the proposed actions.

It was also important to consider whether or not the vignette matrix correlated, therefore a correlation analysis on all 14 questions was performed, comparing the engagement questions and the morality questions on a case by case basis (comparing the engagement variable with the morality variable for the illegal downloading case and so on) as can be seen in Table 8.

**Table 8. Correlations between engagement and morality on a case by case scenario**

	Correlations between engagement and morality	Cronbach's Alpha
Illegal Downloading	$r = -0.33^{***}$	Morality: $\alpha = 0.71$ Engagement: $\alpha = 0.56$
Revenge Porn	$r = -0.39^{***}$	
Cyberbullying	$r = -0.35^{***}$	
Sexting	$r = -0.22^{***}$	
Cyberfraud	$r = -0.21^{***}$	
Cyberstalking	$r = -0.16^{***}$	
Wi-Fi stealing	$r = -0.44^{***}$	

Legend: \*\*\*  $p < 0.001$

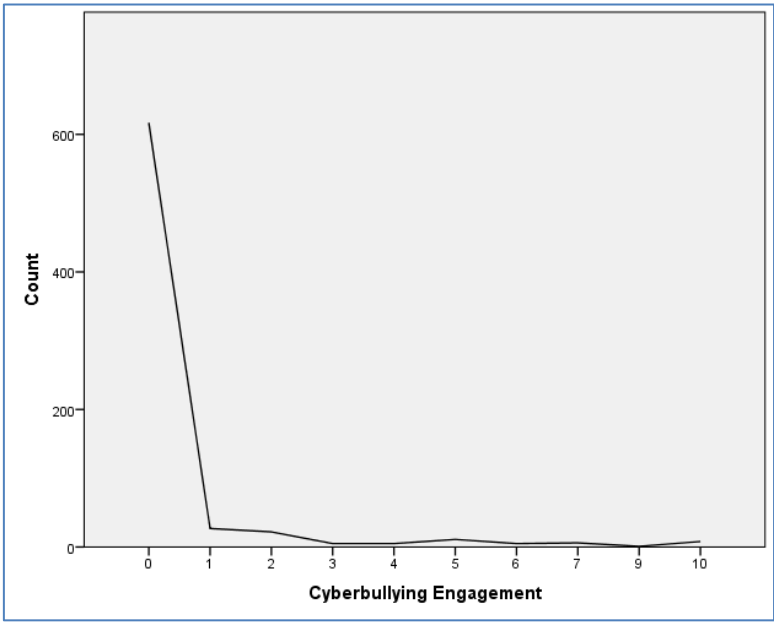
The correlations depicted in Table 8 seem consistent with what has been theorised about the idea of cybercrime propensity. Individuals that would not engage in cybercrime (those leaning



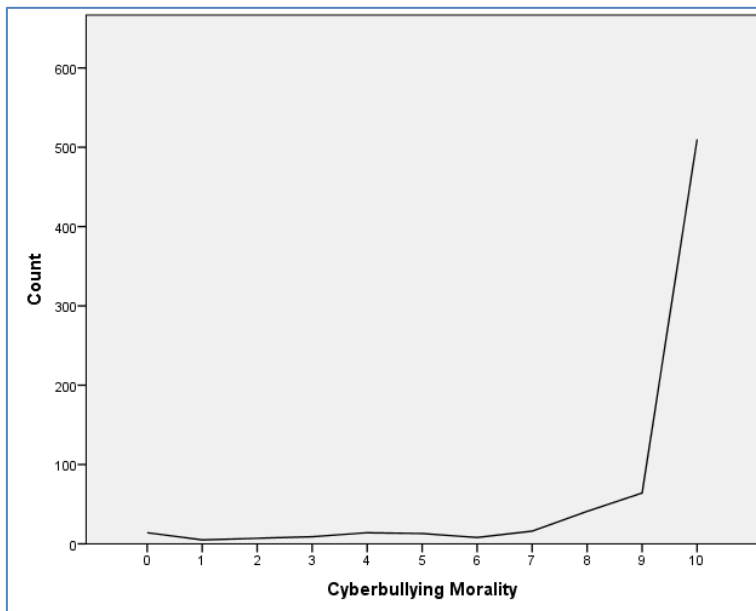
towards the 0 in the engagement question) might understand cybercrime as morally wrong (those leaning towards the 10 in the morality question) and vice-versa, those that would engage in cybercrime might understand it as morally acceptable. The morality questions'  $\alpha=0.706$ , indicated good reliability, on the other hand the engagement questions'  $\alpha=0.562$ , being less reliable.

These negative correlations between pairs can be best seen in a graphic representation in Annex 3 and in Figure 9 and Figure 10.

**Figure 9. Distribution of Cyberbullying Engagement**



**Figure 10. Distribution of Cyberbullying Morality**



In Figures 9 and 10 relating to cyberbullying (see Annex 3 for graphs of each vignette) an almost symmetrical distribution is portrayed. The general pattern that emerged from the elements of propensity (morality and engagement) is that participants that rated a scenario as morally repulsive would not engage in that scenario. Figure 9 demonstrates how individuals lean towards the 0, implying low tendencies to engage in said act).Figure 10 demonstrates that participants understood cybercrime as extremely morally reproachable, as the results lean towards the 10.

#### **4.3.1. Morality**

In terms of correlation, all morality questions correlated positively as seen in Table 9:

**Table 9. Morality correlations**

Morality correlations								
		Illegal Downloading Morality	Revenge Porn Morality	Cyberbullying Morality	Sexting Morality	Cyber Fraud Morality	Cyberstalking Morality	Wi-Fi Stealing Morality
Illegal Downloading Morality	Pearson's correlation	1.00	.12**	.11**	.21**	.10**	.12**	.35**
	Sig. (2-tailed)		.00	.00	.00	.01	.00	.00
	N	707	705	700	706	704	706	707
Revenge Porn Morality	Pearson's correlation	.12**	1.00	.56**	.20**	.53**	.56**	.23**
	Sig. (2-tailed)	.00		.00	.00	.00	.00	.00
	N	705	706	700	705	703	705	706
Cyberbullying Morality	Pearson's correlation	.11**	.56**	1.00	.17**	.55**	.54**	.20**
	Sig. (2-tailed)	.00	.00		.00	.00	.00	.00
	N	700	700	701	700	698	700	701
Sexting Morality	Pearson's correlation	.21**	.20**	.17**	1.00	.19**	.26**	.21**
	Sig. (2-tailed)	.00	.00	.00		.00	.00	.00
	N	706	705	700	706	703	705	706
Cyber Fraud Morality	Pearson's correlation	.10**	.53**	.55**	.19**	1.00	.53**	.19**
	Sig. (2-tailed)	.01	.00	.00	.00		.00	.00
	N	704	703	698	703	705	704	705
Cyberstalking Morality	Pearson's correlation	.12**	.56**	.54**	.26**	.53**	1.00	.22**
	Sig. (2-tailed)	.00	.00	.00	.00	.00		.00
	N	706	705	700	705	704	708	707
Wi-Fi Stealing Morality	Pearson's correlation	.35**	.23**	.20**	.21**	.19**	.22**	1.00
	Sig. (2-tailed)	.00	.00	.00	.00	.00	.00	
	N	707	706	701	706	705	707	708

\*\* . Significance level 0.01 (2-tailed).

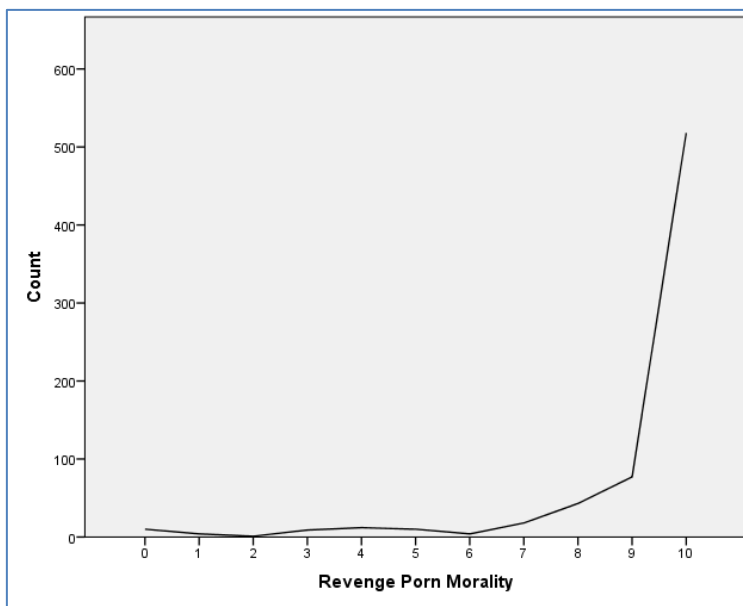
The strongest correlations were found:

- Revenge Porn vignette: Cyberbullying ( $r=0.56$ ), Cyberfraud ( $r=0.53$ ), Cyberstalking ( $r=0.56$ ).
- Cyberbullying vignette: Cyberfraud ( $r=0.55$ ), Cyberstalking ( $r=0.54$ ).
- Cyberfraud vignette: Cyberstalking ( $r=0.53$ ).

All of these correlations were significant at  $p<0.01$ . The cut-off point used for marking a strong correlation point was those higher to  $r=0.50$ .

These correlations seemed to indicate coherence between participant's responses and apparent reliability in the vignettes questions. Participants who have given high scores in a certain vignette (a score of 10 would indicate that they understand the depicted actions as absolutely immoral), would tend to give high scores in some of the others. In other words, there seemed to exist a consensus of sorts in terms of the perception of morality (or more specifically, immorality). Figure 11 might help explaining this tendency.

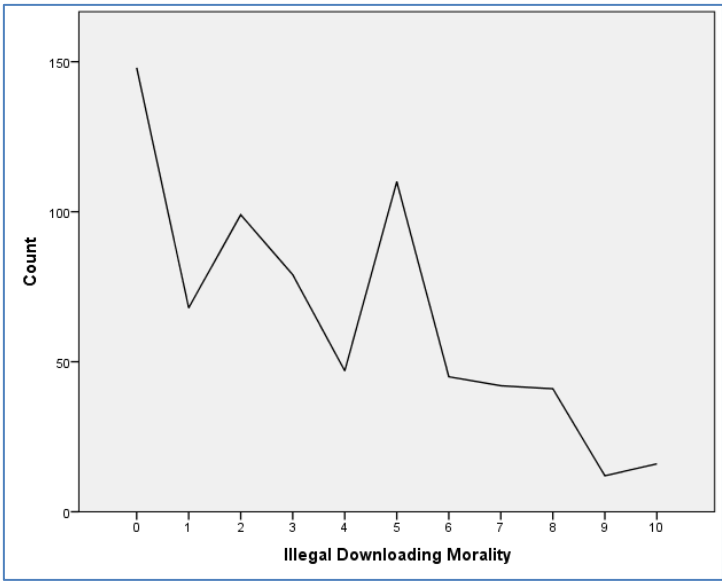
**Figure 11. Distribution of Revenge Porn morality**



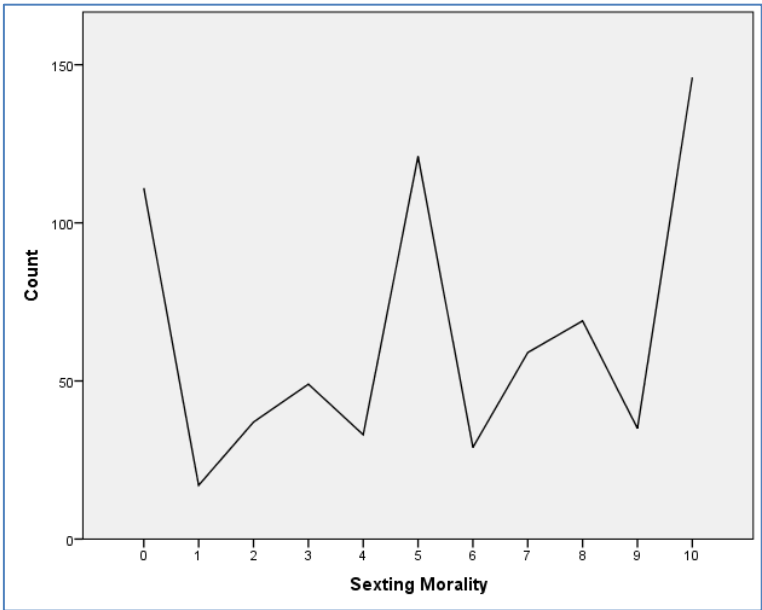
In the vignettes of Revenge Porn (Figure 11) , Cyberbullying, Cyberfraud and Cyberstalking distributions were extremely negatively skewed (see also Annex 3), forming a “precipice of morality” as participants tend to situate themselves at score 10 and regard these behaviours as absolutely immoral. In fact, as it can be observed the mode of all the cases was 10, therefore a very high number of respondents have used the highest scores. For the Revenge Porn vignette,  $M = 9.20$ ; For the Cyberbullying vignette,  $M = 9.03$ ; For the Cyberfraud vignette,  $M = 8.91$ ; For the Cyberstalking vignette,  $M = 8.74$ .

In contrast, in the Illegal Downloading vignette (Figure 12), the Sexting vignette (Figure 13) and the Wi-Fi Stealing vignette (Figure 14) this pattern of the distribution became more erratic. The consensus was, therefore, broken and moral positioning became extremely divergent.

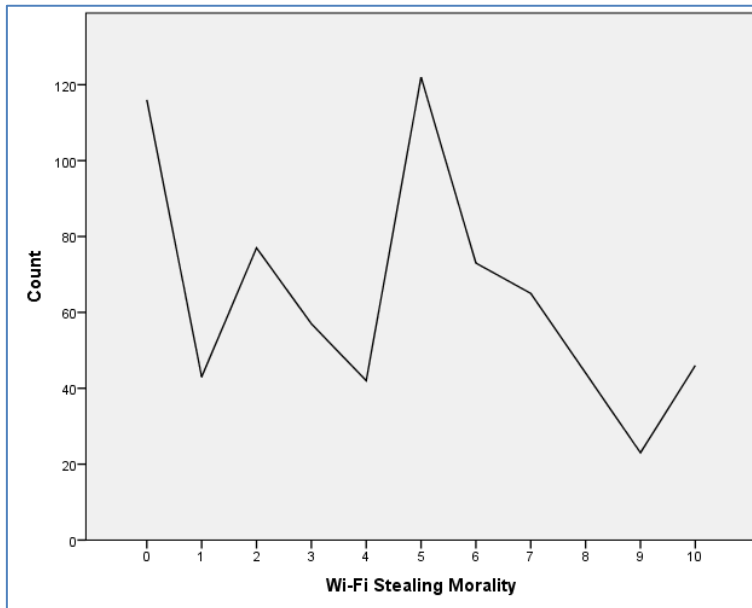
**Figure 12. Distribution of Illegal Downloading Morality**



**Figure 13. Distribution of Sexting Morality**



**Figure 14. Distribution of Wi-Fi Stealing Morality**



For the Illegal Downloading vignette (Fig. 13), for example, the mode = 0, indicating that the majority of people tended to believe that there is nothing immoral in this behaviour. The mean morality score for this hypothetical scenario was 3.40. Therefore, this behavior obtained a moral “pass”. On the other hand, sexting (Fig. 14) was more fluctuating, as the mode =10, the  $M=5.51$  and  $S.D. = 3.48$  (the highest of all different scenarios in terms of morality). Finally, Wi-Fi (Fig. 15) stealing showed mode=5, mean=4.32, and  $S.D. =3.02$  (the second highest deviation).

In relation to the victim of crime variable, several T-Tests demonstrated that there was not a statistically significant relationship between whether or not the participant had been a victim of crime and the perceptions of morality. In the case of illegal downloading, the means for the victim and non-victim group were both 3.40. In this case the *alpha value* was almost equal to 1, therefore there is strong evidence to validate the null hypothesis, relating to the

independence of the variables. In other vignettes, like Revenge Porn and Cyberbullying, alpha was also extremely close to 1.

**Table 10. Morality questions means' comparisons by gender and victimhood**

	Gender	Victim of Crime
Illegal Downloading Morality	t(705)=2.07*	t(704)=-0.00
Revenge Porn Morality	t(704)=-3.50***	t(703)=0.22
Cyberbullying Morality	t(699)=-2.85**	t(698)=0.20
Sexting Morality	t(704)=-1.12	t(703)=-0.67
Cyberfraud Morality	t(703)=-1.98*	t(702)=0.66
Cyberstalking Morality	t(706)=-0.31	t(705)=-0.61
Wi-Fi stealing Morality	t(706)=-1.74	t(705)=-1.66

Legend: \* p<0.05/ \*\* p<0.01/\*\*\* p<0.001

In relation to gender, it was shown previously that there is a significant relationship between perceptions of morality and gender in the Revenge Porn vignette ( $p<0.001$ , being the negative *t-value* the highest of them all). Also, the Cyberbullying Case ( $t(699) = -2.85$ ,  $p<0.01$ ); the Illegal Downloading vignette and the Cyberfraud vignette showed  $p<0.05$ . However, the Sexting vignette, the Wi-Fi Stealing vignette and the Cyberstalking vignette showed no statistical significance after the T-Tests were performed (all cases  $p>0.05$ ; for the Cyberstalking Case,  $p=0.76$ ). Even though, the means for women were slightly higher than the means for men (with the exception of illegal downloading where said trend is reversed). It is worth mentioning that women rated the scenarios as more morally reproachable than men, with the exception of Illegal Downloading, that was understood as more morally reproachable by men (women,  $n=400$ ,  $M=3.21$ ; men,  $n=307$ ,  $M=3.64$ ).



The six different elements of self-control (Impulsivity, Simple Tasks, Risk Seeking, Physical activities, Egotism, Temper) were analysed in relation to the perceptions of morality in the different scenarios. After this, the results of several T-Tests were also analysed in relation to the aggregated self-control variable and the different perceptions of morality, scenario by scenario.

In order to compare the means between perceptions of morality and self-control (not being dichotomous variables), two groups within the morality variables were created for T-Testing. The “precipice” of morality was taken into account (the majority of answers lean towards the 10, producing an extremely steep curve). T-Tests were performed with two new independent samples utilizing a cut point: comparing the means of the participants who scored 10 against those who scored less than 10. Table 11 shows the results of these T-Tests.

**Table 11. The six elements of self-control mean's comparisons by perceptions of morality**

	Illegal Downloading	Revenge Porn	Cyberbullying	Sexting	Cyber Fraud	Cyber Stalking	Wi-Fi stealing
<b>Impulsivity</b>	t(696)=1.07	t(695)=-2.97**	t(690)=-3.80***	t(695)= 0.35	t(694)=-3.35**	t(697)=-2.87**	t(697)=-1.07
<b>Simple Tasks</b>	t(697)=-0.56	t(696)=-5.29***	t(691)=-4.52***	t(696)=-1.15	t(695)=-3.56***	t(698)=-4.16***	t(698)=-2.60**
<b>Risk Seek</b>	t(697)=-2.21*	t(696)=-4.29***	t(691)=-5.54***	t(696)=-2.12*	t(695)=-5.20***	t(698)=-3.89***	t(698)=-2.49*
<b>Physical Activities</b>	t(691)=0.70	t(689)=-0.93	t(684)=-0.94	t(690)=1.68	t(688)=-1.28	t(691)=0.80	t(691)=-0.59
<b>Egotism</b>	t(692)=1.13	t(690)=-5.16***	t(685)=-5.75***	t(691)=-0.51	t(689)=-5.86***	t(692)=-3.18**	t(692)=-2.48*
<b>Temper</b>	t(698)=-0.02	t(697)=-3.06**	t(692)=-2.63**	t(697)=-0.47	t(696)=-2.30*	t(699)=-2.45*	t(699)=-0.98

Legend: \* p<0.05/ \*\*p<0.01/\*\*p<.001

One of the problems that arose when considering the results of the T-Tests, is that sample sizes were extremely unbalanced in the Wi-Fi Stealing and the Illegal Downloading vignettes. This is due to the fact that few participants chose 10 (the absolute moral reproachability score) for these cases, with the vast majority giving rankings less than 10.

After comparing the means, the physical activities element (variable) showed no statistical significance in relation to any of the cybercrime vignettes (see Table 12). It seemed that the liking for physical activities amongst the sample was not related to their perceptions of morality. The reason for this might lie in the fact that cybercrime requires almost no physical effort (beyond clicking buttons and writing e-mails, for example) as opposed to other types of crimes (such as burglaries, robberies and assaults), which require more intense physical engagement. However, this element should be considered in the aggregated measures of self-control, even though it seems to hold no meaning if considered in itself.

On the other hand, perceptions of morality for Revenge Porn, Cyberbullying, Cyberfraud and Cyberstalking demonstrated statistical significance in relation to all of the other five elements (except physical activities). In other words, people that rated these vignettes with a score of 10 (absolutely immoral), showed lower means of impulsivity, egotism, risk seeking traits, temperamental attitudes and preference for simple tasks.

Two exceptions to the overall trend emerged: Sexting and Illegal Downloading. The morality variable of the Sexting vignette was only significant in relation to risk seeking tendencies, demonstrating that the sample that rated sexting as absolutely immoral had lower means of risk seeking tendencies. This could be explained on the basis of the way in which the case was

formulated (a younger girl starting a relationship with an older man hiding behind a false identity) as it could imply the idea of risk-taking and somewhat reckless behaviour on the part of the victim. The very same pattern occurred with illegal downloading and risk-seeking, as the only significant comparison between means indicates that the sample that rated Illegal Downloading as absolutely immoral, scored lower in the risk-seeking mean (see Table 11). Should, therefore, illegal downloading be conceived as a risk-based activity? There does not seem to be enough data to support this premise, especially given that the group which rated illegal downloading as absolutely immoral is very small compared to the group which rated illegal downloading as moral. These unbalanced distributions of samples could breach the assumptions of normality within the T-Test and produce biased results (Field, 2009, p.345; citing Wilcox, 2005).

Finally, a comparison between the means of the perceptions of morality for each vignette and the aggregated self-control interval variable and self-control dichotomous variable was carried out (Table 12). These findings are key to the theoretical model being developed in this thesis; a model that seeks to relate self-control to propensity and the use of neutralisation techniques. Once again, in order to compare the means, two independent samples were created one for morality scores equal to 10 (absolutely immoral) and another one for morality scores below 10 (below absolutely immoral). All negative *t-values* were significant at  $p < 0.01$  and  $p < 0.001$  with the exception of the sexting and illegal downloading scenarios. The group that tended to rate the vignettes as absolutely immoral, demonstrated lower means of self-control (indicating, therefore, higher levels of self-control).

**Table 12. Self-control means' comparisons by morality questions**

	Self-Control (Morality=10/Morality <10)	Self-Control (High/Low)
Illegal Downloading	t (659) = -0.40	t (659) = 2.17*
Revenge Porn	t (657) = -4.86***	t (657) = 4.20***
Cyberbullying	t (652) = -5.596***	t (652) = 3.46**
Sexting	t (658) = -0.43	t (658) = -0.32
Cyber Fraud	t (656) = -5.19***	t (656) = 4.29***
Cyber Stalking	t (659) = -3.70***	t (659) = 1.60
Wi-Fi Stealing	t( 659)= -2.79**	t (659) = 2.53*

Legend: \* p<0.05/ \*\* p<0.01/ \*\*\* p<0.001

For the Sexting vignettes, the means were similar, indicating that self-control does not play a part in rating the sexting case morally. Something similar emerged in regards to the Illegal Downloading vignette, bearing in mind that only n=13, as opposed to n=648, rated this behavior as absolutely immoral. Illegal downloading seemed to be embedded in the *habitus* of the sample, something so utterly natural in today's society that is not regarded as immoral.

Another set of T-Tests were performed (from a different perspective, see also Table 12), using Self-Control (High/Low) as the grouping variable and the perceptions of morality as variables for contrasting, in order to compare the means for morality. All *t-values* were positive and statistically significant, with the exception of the sexting case that showed the lowest negative *t-values* and the cyberstalking case that had a low positive *t-value*. For every vignette, the High Self-Control Sample showed higher means of perceptions of morality (for them the vignettes were more immoral) than the Low Self-Control Sample. In the sexting case both means were extremely similar (morally "lukewarm") and in the Cyberstalking vignette were means were extremely similar (moral "fail"). This seemed to demonstrate that higher scores of self-control are related to higher scores of morality (leaning towards the moral "fail"). Therefore, participants with high self-control understood cybercrimes as more immoral, than participants with low self-control. This rule is, once again, proven wrong for the sexting case which is understood as morally indifferent, regardless of the level of self-control

The reason why the Cyberstalking means were similar between both samples of low and high self-control is unclear, yet it shows a similar pattern to the one encountered when using gender as the grouping variable. It must be noted that even though high self-control was found more in women than men, the means for the Cyberstalking vignette were similar regardless of gender. Both men and women, and people with high and low self-control rated Cyberstalking above 8 in terms of morality (moral “fail”).

In terms of correlations between the morality and engagement questions, they generally correlated. The following (marked in darker colour in Table 13) are the ones that did not correlate (only referring to not correlating between the engagement and the morality questions, not the morality questions with the morality questions or the engagement questions with the engagement questions).

**Table 13. Engagement and morality correlations**

Morality and Engagement correlations																
		Illegal Downloading Engagement	Revenge Pom Engagement	Cyberbullying Engagement	Sexting Engagement	Cyberfraud Engagement	Cyberstalking Engagement	Wi-Fi Stealing Engagement	Illegal Downloading Morality	Revenge Pom Morality	Cyberbullying Morality	Sexting Morality	Cyberfraud Morality	Cyberstalking Morality	Wi-Fi Stealing Morality	
Illegal Downloading Engagement	Pearson's correlation	1.00	.05	.03	.05	.03	.06	.44	-.33	.13	.07	-.02	.07	.08	-.12	
	Sig. (2-tailed)		.22	.41	.23	.42	.12	.00	.00	.00	.05	.65	.05	.03	.00	
	N	707	702	706	704	704	704	707	706	705	700	705	704	706	707	
Revenge Pom Engagement	Pearson's correlation	.05	1.00	.22	.13	.22	.22	.10	-.01	-.39	-.07	.01	-.07	-.04	-.11	
	Sig. (2-tailed)	.22		.00	.00	.00	.00	.01	.83	.00	.06	.73	.05	.25	.00	
	N	702	704	703	702	701	701	704	703	703	698	703	700	703	703	
Cyberbullying Engagement	Pearson's correlation	.03	.22	1.00	.17	.38	.37	.07	.04	-.09	-.35	.08	-.07	-.10	.02	
	Sig. (2-tailed)	.41	.00		.00	.00	.00	.06	.24	.01	.00	.05	.05	.01	.67	
	N	706	703	707	705	704	704	707	706	706	701	706	704	706	707	
Sexting Engagement	Pearson's correlation	.05	.13	.17	1.00	.28	.31	.11	.00	-.03	-.07	-.22	-.06	-.05	-.05	
	Sig. (2-tailed)	.23	.00	.00		.00	.00	.00	.94	.40	.06	.00	.12	.21	.19	
	N	704	702	705	705	702	702	705	705	704	699	705	702	704	705	
Cyberfraud Engagement	Pearson's correlation	.03	.22	.38	.28	1.00	.50	.13	.03	-.13	-.07	.05	-.21	-.09	-.01	
	Sig. (2-tailed)	.42	.00	.00	.00		.00	.00	.47	.00	.08	.15	.00	.02	.72	
	N	704	701	704	702	706	703	706	704	703	698	703	703	705	705	
Cyberstalking Engagement	Pearson's correlation	.06	.22	.37	.31	.50	1.00	.09	.06	-.08	-.10	.06	-.07	-.16	.04	
	Sig. (2-tailed)	.12	.00	.00	.00	.00		.01	.09	.03	.01	.09	.06	.00	.31	
	N	704	701	704	702	703	706	706	704	703	698	703	702	705	705	
Wi-Fi Stealing Engagement	Pearson's correlation	.44	.10	.07	.11	.13	.09	1.00	-.22	.11	.06	-.01	.09	.01	-.44	
	Sig. (2-tailed)	.00	.01	.06	.00	.00	.01		.00	.00	.09	.76	.02	.74	.00	
	N	707	704	707	705	706	706	709	707	706	701	706	705	708	708	
Illegal Downloading Morality	Pearson's correlation	-.33	-.01	.04	.00	.03	.06	-.22	1.00	.12	.11	.21	.10	.12	.35	
	Sig. (2-tailed)	.00	.83	.24	.94	.47	.09	.00		.00	.00	.00	.01	.00	.00	
	N	706	703	706	705	704	704	707	707	705	700	706	704	706	707	
Revenge Pom Morality	Pearson's correlation	.13	-.39	-.09	-.03	-.13	-.08	.11	.12	1.00	.56	.20	.53	.56	.23	
	Sig. (2-tailed)	.00	.00	.01	.40	.00	.03	.00	.00		.00	.00	.00	.00	.00	
	N	705	703	706	704	703	703	706	705	706	700	705	703	705	706	
Cyberbullying Morality	Pearson's correlation	.07	-.07	-.35	-.07	-.07	-.10	.06	.11	.56	1.00	.17	.55	.54	.20	
	Sig. (2-tailed)	.05	.06	.00	.06	.08	.01	.09	.00	.00		.00	.00	.00	.00	
	N	700	698	701	699	698	698	701	700	700	701	700	698	700	701	
Sexting Morality	Pearson's correlation	-.02	.01	.08	-.22	.05	.06	-.01	.21	.20	.17	1.00	.19	.26	.21	
	Sig. (2-tailed)	.65	.73	.05	.00	.15	.09	.76	.00	.00	.00		.00	.00	.00	
	N	705	703	706	705	703	703	706	706	705	700	706	703	705	706	
Cyberfraud Morality	Pearson's correlation	.07	-.07	-.07	-.06	-.21	-.07	.09	.10	.53	.55	.19	1.00	.53	.19	
	Sig. (2-tailed)	.05	.05	.05	.12	.00	.06	.02	.01	.00	.00	.00		.00	.00	
	N	704	700	704	702	703	702	705	704	703	698	703	705	704	705	
Cyberstalking Morality	Pearson's correlation	.08	-.04	-.10	-.05	-.09	-.16	.01	.12	.56	.54	.26	.53	1.00	.22	
	Sig. (2-tailed)	.03	.25	.01	.21	.02	.00	.74	.00	.00	.00	.00	.00		.00	
	N	706	703	706	704	705	705	708	706	705	700	705	704	708	707	
Wi-Fi Stealing Morality	Pearson's correlation	-.12	-.11	.016	-.049	-.013	.038	-.441	.345	.227	.196	.210	.191	.223	1	
	Sig. (2-tailed)	.00	.00	.668	.192	.722	.313	.000	.000	.000	.000	.000	.000	.000		
	N	707	703	707	705	705	705	708	707	706	701	706	705	707	708	
**. Significance level 0.01 (2-tailed).																
*. Significance level 0.05 (2-tailed).																

Once again, the Illegal Downloading vignette, the Sexting vignette and the Wi-Fi Stealing vignette did not generally follow the overall patterns that emerged from the data. The majority of participants rated vignettes by using extreme scores, thus creating a precipice of morality and engagement in terms of their distribution. However, for Illegal Downloading, Sexting or Wi-Fi Stealing this tendency is different or even reversed, as participants seemed to present different and contrasting moral views or indicated the likelihood of committing these actions (which might not be understood as cybercriminal by the sample).

#### **4.3.2. Engagement**

This variable was formatted as a “Would you do what someone did?” question. Morality and engagement measure the propensity of the individual for the commission of cybercrime, and were correlates with one another as indicated above. Someone understanding certain behaviour as morally wrong would not engage (theoretically) in said behaviour. It is important to take into consideration that the questionnaire measured propensity in a projective way, meaning that it is not a self-report questionnaire on whether or not participants had committed any anti-normative cyber-activity. Therefore, perceptions of morality and engagement should form a consistent moral framework for the measure of propensity within the sample.

In terms of correlations between the different engagement questions see Table 14.



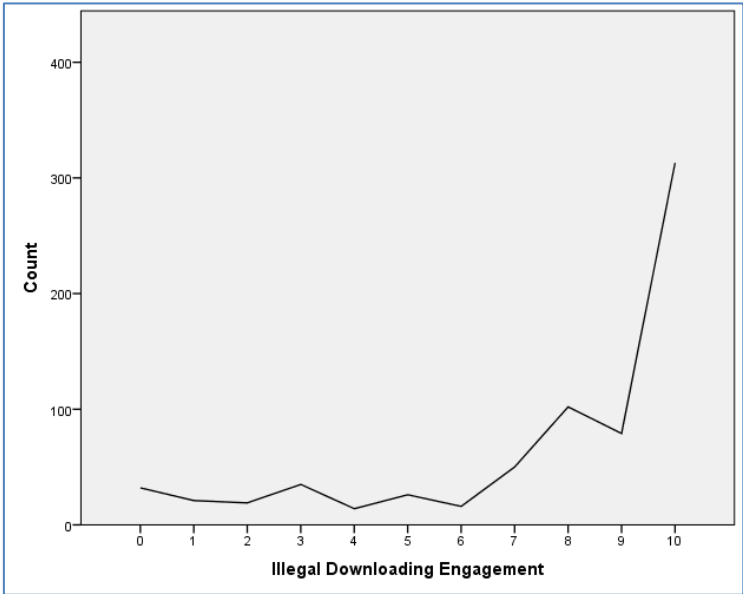
**Table 14. Engagement questions correlations**

Engagement correlations								
		Illegal Downloading Engagement	Revenge Porn Engagement	Cyberbullying Engagement	Sexting Engagement	Cyberfraud Engagement	Cyberstalking Engagement	Wi-Fi Stealing Engagement
Illegal Downloading Engagement	Pearson's correlation	1.00	.05	.03	.05	.03	.06	.44**
	Sig. (2-tailed)		.22	.41	.23	.42	.12	.00
	N	707	702	706	704	704	704	707
Revenge Porn Engagement	Pearson's correlation	.05	1.00	.22**	.13**	.22**	.22**	.10**
	Sig. (2-tailed)	.22		.00	.00	.00	.00	.01
	N	702	704	703	702	701	701	704
Cyberbullying Engagement	Pearson's correlation	.03	.22**	1.00	.17**	.38**	.37**	.07
	Sig. (2-tailed)	.41	.00		.00	.00	.00	.06
	N	706	703	707	705	704	704	707
Sexting Engagement	Pearson's correlation	.05	.13**	.17**	1.00	.28**	.31**	.11**
	Sig. (2-tailed)	.23	.00	.00		.00	.00	.00
	N	704	702	705	705	702	702	705
Cyberfraud Engagement	Pearson's correlation	.03	.22**	.38**	.28**	1.00	.50**	.13**
	Sig. (2-tailed)	.42	.00	.00	.00		.00	.00
	N	704	701	704	702	706	703	706
Cyberstalking Engagement	Pearson's correlation	.06	.22**	.37**	.31**	.50**	1.00	.09*
	Sig. (2-tailed)	.12	.00	.00	.00	.00		.01
	N	704	701	704	702	703	706	706
Wi-Fi Stealing Engagement	Pearson's correlation	.44**	.10**	.07	.11**	.13**	.09*	1.00
	Sig. (2-tailed)	.00	.01	.06	.00	.00	.01	
	N	707	704	707	705	706	706	709

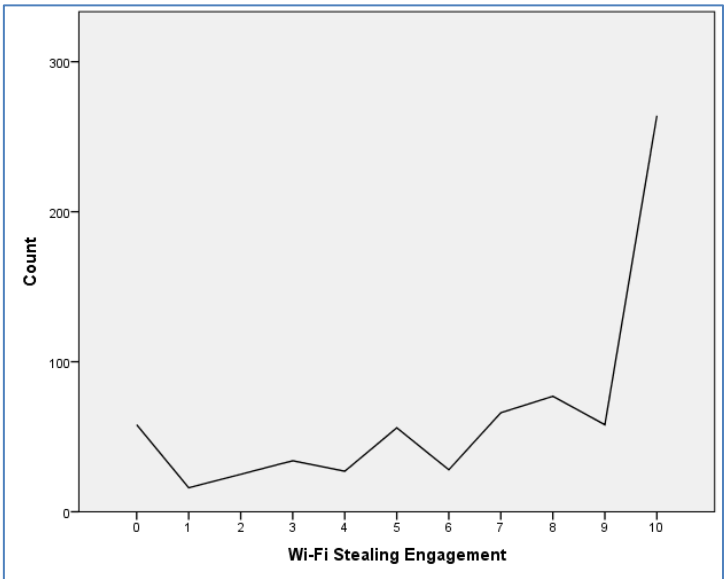
\*\* . Significance level 0.01 (2-tailed).  
 \* . Significance level 0.05 (2-tailed).

The Illegal Downloading vignette did not correlate significantly with any other vignette except Wi-Fi stealing. Moreover, the correlation between Illegal Downloading and Wi-Fi Stealing was the strongest ( $r=0.44$ ) of all. Similarly, the Wi-Fi stealing vignette did not correlate significantly with the Cyberbullying vignette or the Cyberstalking vignette.

**Figure 15. Distribution of engagement in Illegal Downloading**



**Figure 16. Distribution of engagement in Wi-Fi Stealing**

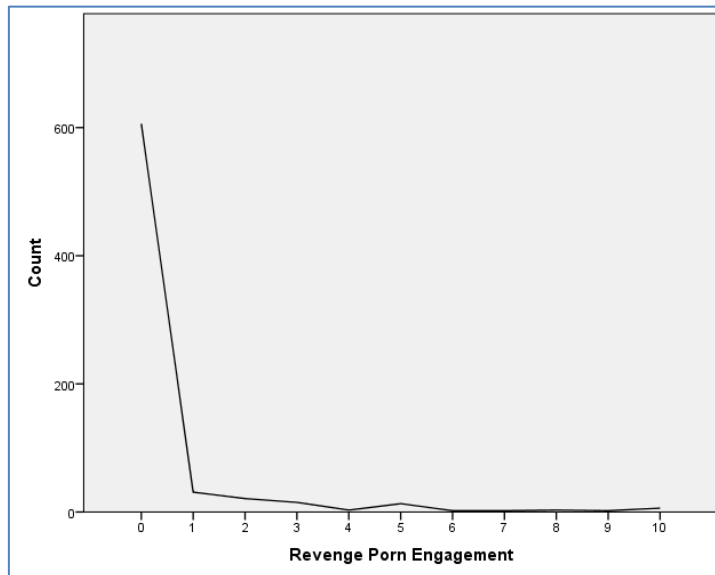


In order to understand these correlations, an analysis of each scenario was needed. In Figures 15 and 16, the similarities of between the distribution of the illegal Downloading vignette and the Wi-Fi Stealing vignette can be easily observed. In the Illegal Downloading vignette ((N=702) M=7.71, mode=10 and S.D. =3.03) and Wi-Fi Stealing vignette ((N=709), M= 7, mode=10 and S.D.=3.31) the means were high, indicating that participants would engage in the behaviours depicted . Both cases were negatively skewed and form another “precipice” similar to the one found in the majority of morality cases, yet different to all other engagement distributions. Both cases have also shown the highest dispersion and break the “consensus” that occurred around the other scenarios. In other words, the majority of participants would engage in Illegal Downloading and Wi-Fi Stealing. It should be noted that the mode was situated in 10, therefore the majority of participants were in absolute agreement with the idea of committing these cybercrimes. However, this does not mean they would necessarily have done so but rather that there was a high likely that they would do so. At the very same time, both vignettes have obtained a moral “pass”. The study of neutralisation techniques became crucial to understanding this phenomenon.

In relation to all the other vignettes (Annex 3) the “precipice” was inverted and positively skewed. All of the modes=0, the means were less than 1 and the S.D. lower than they were for the Illegal Downloading and the Wi-Fi Stealing scenarios. The majority of participants would not do what is depicted in any of the other vignettes (Revenge Porn, Cyberbullying, Cyberfraud, Cyberstalking and Sexting). All of the remaining scenarios, with the exception of sexting, referred to situations of abuse and victimization that are also criminal in the Spanish legal system. A sample with high levels of self-control should not accept crime as a viable alternative. It was not possible, however, to ascertain whether or not participants have engaged in any of these activities (not even the Illegal Downloading or Wi-Fi stealing ones) or

whether or not a social desirability bias has occurred. The idea of participants answering in a hypothetical fashion might have shielded the questionnaire against the occurrence of said bias.

**Figure 17. Distribution of engagement in Revenge Porn**



It is important to mention that, as theorized, there was coherence and congruency between measures of propensity (engagement and morality), as generally speaking participants would only engage in acts that they deem as morally appropriate or acceptable. The only exception was the Sexting vignette ( $M = 0.90$ ; mode=0, S.D. =2.08). First, it is the third scenario with the highest dispersion (after Illegal Downloading and the Wi-Fi Stealing one). Secondly, participants tended to be in absolute disagreement with the idea of engaging in Sexting yet they have rated it as morally “lukewarm” (in terms of morality, mode =10,  $M=5.51$  and S.D. = 3.48). Sexting was the exception again, as it was the only case where, even though participants had very mixed views on its morality, and it was not really rated as right or wrong, they would not engage in it. It must said once again that engagement and morality correlated negatively ( $r= -0.22$ ,  $p<0.001$ ) in the Sexting vignette.

As indicated in previous paragraphs, participants who rated sexting as morally reproachable, exhibited a lower mean for risk-seeking tendencies. In contrast (and this is explained, in detail, below) those who were less likely to engage in Sexting, showed a lower mean for risk-seeking tendencies. Both results were statistically significant.

In relation to the victimization status variable, several T-Tests demonstrated that there was no statistically significant relationship between whether or not the participant has been a victim of crime and the engagement variable. The sole exception was the Sexting vignette ( $t(702) = 3.09$ ,  $p < 0.01$ ). The victimisation status did not show any statistical significance after performing T-Tests and *chi-square* tests, and it did not seem to have any relationship with, gender self-control measures, morality and now the engagement variable. The results of the T-Tests can be seen in Table 15.

**Table 15. Engagement means' comparisons by gender and victimhood.**

	Gender	Victim of Crime
Illegal Downloading Engagement	$t(705) = -1.10$	$t(704) = 0.63$
Revenge Porn Engagement	$t(702) = 4.63^{***}$	$t(701) = -0.38$
Cyberbullying Engagement	$t(705) = 3.46^{**}$	$t(704) = 0.19$
Sexting Engagement	$t(703) = 4.80^{***}$	$t(702) = 3.09^{**}$
Cyber Fraud Engagement	$t(704) = 2.53^*$	$t(703) = 1.52$
Cyber Stalking Engagement	$t(704) = 3.10^{**}$	$t(703) = 1.57$
Wi-Fi stealing Engagement	$t(707) = -0.67$	$t(706) = 1.76$

Legend: \*  $p < 0.05$ / \*\*  $p < 0.01$ / \*\*\*  $p < 0.001$

In relation to the Sexting vignette, the means were not very different from one another (respondents answering Yes:  $n=220$ ,  $\text{mean}=1.26$ ; respondents answering No:  $n=484$ ,  $\text{mean}=0.74$ ) as both would not engage in sexting activities, although the ones that have been victimized were, in contrast, slightly more prone to take part in Sexting.

In terms of gender the relationship was statistically significant, with the exception of the Illegal Downloading and the Wi-Fi Stealing vignette. In the Revenge Porn vignette, Cyberbullying vignette, Sexting vignette and Cyberstalking vignette all  $p<0.01$  and  $p<0.001$  with positive *t-values*, whilst the Cyberfraud vignette  $p<0.05$ . Males showed higher means in the engagement variable than women, meaning that men were more likely to engage in said acts. Male participants tended to rate vignette as less morally reproachable than women, with the exception of Illegal Downloading and Wi-Fi Stealing where the tendency was inverted. (However, Illegal Downloading and Wi-Fi Stealing showed no statistical significance in relation to morality means by gender). Recalling the findings that men also had lower levels of self-control, it appears that there was congruent relationship between self-control, morality and engagement, and that men demonstrated more propensity towards cybercrime. What needs to be addressed is the reason why both males and females rated sexting as morally “lukewarm”, without any significant differences in their means, yet males were significantly more likely to engage in sexting. This could be because men are more prone to risk-seeking activities, as opposed to women who exercise more self-control. In a T-Test that used gender as the grouping variable, to compare the risk-seeking means, the results demonstrated that men score higher in risk-seeking tendencies ( $t(699)=4.98$ ;  $p<0.001$ ). Sexting engagement is very significantly linked to the risk-seeking element of self-control.

In the Illegal Downloading vignette and the Wi-Fi vignette where  $p > 0.05$ , the *t-values* were negative and the mean comparison indicated inversely that women were slightly more likely to engage in Illegal Downloading or Wi-Fi Stealing.

The six different elements of self-control were analysed and subsequently the self-control aggregated interval variable and the self-control (High/Low) dichotomous variable. In order to compare the elements of self-control, two samples were created from the engagement variable. Using a similar (yet inverse) pattern to the one from the morality variable epigraph, two independent self-control sub-samples were generated by using a cut point that separated those ranking the “would you do it?” questions with a naught score and those that ranked higher. Note that the mode of the engagement cases was usually equal to naught.

**Table 16. The six elements of self-control mean's comparisons by engagement**

	Illegal Downloading	Revenge Porn	Cyberbullying	Sexting	Cyberfraud	Cyberstalking	Wi-Fi stealing
<b>Impulsivity</b>	t(696)=2.88**	t(693)=4.84***	t(696)=4.80***	t(694)=4.10***	t(695)=4.33***	t(695)=5.71***	t(698)=2.10*
<b>Simple Tasks</b>	t(607)=2.26*	t(694)=5.87***	t(697)=4.12***	t(695)=2.83**	t(696)=5.12***	t(696)=5.09***	t(699)=3.11**
<b>Risk Seek</b>	t(697)=1.59	t(694)=6.74***	t(697)=4.87***	t(695)=5.74***	t(696)=5.97***	t(697)=4.74***	t(699)=2.86**
<b>Physical Activities</b>	t(690)=1.97*	t(688)=4.17***	t(690)=2.62**	t(689)=0.80	t(690)=3.24**	t(689)=1.61	t(692)=0.81
<b>Egotism</b>	t(691)=0.73	t(689)=6.88***	t(691)=5.74***	t(690)=4.48***	t(690)=6.95***	t(690)=4.99***	t(693)=1.50
<b>Temper</b>	t(698)=3.39**	t(695)=5.34***	t(698)=3.90***	t(696)=1.24	t(697)=3.87***	t(697)=4.44***	t(700)=2.27*

Legend: \* p<0.05/ \*\*p<0.01/\*\*\* p<.001



In these T-Tests (Table 16), the Illegal Downloading vignette was not statistically significant in relation to the Egotism and the Risk-Seeking elements. On the other hand, Sexting was not significant only in relation to Temper and Physical Activities. Subsequently, it was found that the engagement variable seemed to be more profoundly related to the different elements of self-control than the perceptions of morality. These six elements seemed, therefore, crucial in determining whether or not people would engage in the cybercriminal activities presented in the questionnaire. Also, even though the Physical Activity element played (see Table 11) no part in the perceptions of morality, there was a significant statistical relationship with Illegal Downloading, Revenge Porn, Cyberbullying and Cyberfraud.

If the aggregated self-control variable (Table 17) is taken into consideration (by using it as grouping variable with two sub-samples), this statistical significance became more apparent. Given that all of the engagement variables had demonstrated a significant relationship with self-control.

**Table 17. Self-control means' comparisons by engagement questions**

	Self-Control (Engagement=0/Engagement <0)	Self-Control (High/Low)
Illegal Downloading	t(658)= 3.10**	t (658)= -2.91**
Revenge Porn	t(656) = 8.14***	t (656)= -5.02***
Cyberbullying	t(658) =6.00***	t (658)= -3.90***
Sexting	t(657) = 4.36***	t (657)= -1.44
Cyberfraud	t(658)= 6.91***	t (658) = -5.59***
Cyberstalking	t(658)= 5.94***	t(658)= -2.56*
Wi-Fi Stealing	t(660)= 3.09**	(660)= -3.05**

Legend: \* p<0.05/ \*\*p<0.01/\*\*\* p<.001

The process used for carrying out the T-Tests, was not dissimilar to the one used for the perceptions of morality. Two independent samples were created from each engagement variable, taking into consideration the “precipice” distribution. Given that all of the modes=0 and the means were less than 1, with the exceptions of the Illegal Downloading vignette and the Wi-Fi Stealing vignette. In order to T-Test each, for each vignette, two sub-samples were created: those scoring 0 and sample 2: those scoring more than 0. Self-control proved to be statistically significant for every single case, with high positive *t-values* (for example, Cyberstalking=5.94; Cyberfraud= 6.91; Cyberbullying=5.94; Revenge Porn=8.14).

In terms of means, the samples that rated engagement with 0 (meaning that they would never partake in such an activity) showed lower means of self-control (therefore they displayed higher levels of self-control), whereas participants that rated engagement with more than 0 showed higher mean of self-control (therefore displaying lower levels of self-control). One of the major problems that arose during the comparison was the imbalance of the two independent samples:

- Revenge Porn: Sample 1: n=566, Sample 2: n=92
- Cyberbullying: Sample 1: n=575, Sample 2: n=85
- Sexting: Sample 1: n=514, Sample 2: n=145
- Cyberfraud: Sample 1: n=578, Sample 2: n=82
- Cyberstalking: Sample 1: n=567, Sample 2: n=93

In contrast, the Illegal Downloading and the Wi-Fi Stealing cases were imbalanced in a different fashion due to the fact that the majority of participants were in favour of said activities.

- Illegal Downloading: Sample 1: n=30, Sample 2: n= 630
- Wi-Fi Stealing: Sample 1: n= 55, Sample 2: n=607

When the SelfControl\_HighLow (also in Table 17) categorical variable was considered as a grouping variable, and all of the engagement questions' means compared by using a T-Test, the following was found: all the *t-values* are negative. People with low self-control considered themselves as more likely to engage in acts of cybercrime. In all of these cases, the samples were also imbalanced as the majority of respondents were members of the High Self-Control sample.

Both systems of T-Testing (by using SelfControlHighLow as the grouping variable or by creating two independent samples in the engagement variables by means of a cut point) gave identical results with the exception of the Sexting vignette (a similar incongruence was also found when analysing the morality variables).

### 4.3.3. Neutralisation techniques

The questionnaire was designed for participants to pick as many neutralisations as they deemed necessary for each case, in order to constrain them as less as possible. However, the possibility of participants picking “It’s not justifiable” plus any other neutralisation was not forestalled. Given that the researcher designed the questionnaire by understanding “unjustifiable” as the complete absence of neutralisations. Some other participants did not pick any neutralisation technique at all. After some discussion with the PhD supervisors, it was decided that all the respondents that picked “unjustifiable” and other neutralisations, and all the respondents that did not pick any neutralisation, were retained in order to fully understand the psychological makeup of the sample. Some reliability issue may have arisen. Table 18 is a summary of the inconsistencies found in the neutralisation techniques variables.

**Table 18. Inconsistencies found when coding neutralisation techniques answers**

	No neutralisation techniques picked	Unjustified+ other neutralisation techniques
Illegal Downloading	6	18
Revenge Porn	7	32
Cyberbullying	11	18
Sexting	6	16
Cyberfraud	6	24
Cyberstalking	5	14
Wi-Fi Stealing	2	14

For example, as can be seen in Table 18, 32 respondents picked the “it’s not justified” technique and other techniques in the Revenge Porn vignette. This vignette is the one where this inconstancy appeared most. On the other hand, 11 respondents did not pick any neutralisation techniques in the Cyberbullying vignette.

In Table 19, the frequencies of all the neutralisation techniques on a case by case scenario are explained. For each vignette, the three most frequent techniques have been coloured. The choices changed between vignettes, however, “it’s not justifiable” and “nothing wrong” appeared quite frequently.

**Table 19. Frequencies of neutralisation techniques**

	Unjustifiable	Nothing Wrong	Not My Fault	Victim's Fault	Everyone	No Other Choice	It's My Right	Ledger
Illegal Downloading	17.3 %	21.4%	4.5 %	8.6 %	34.4 %	19 %	11. 6%	8%
Revenge Porn	68.7%	1.4%	2%	30%	0.4 %	2.1 %	5.1 %	1 %
Cyberbullying	71. 7 %	10. 7%	2.3%	5. 9 %	10.9 %	0.7%	3.8%	6.8%
Sexting	25.7%	43 %	2.5 %	1.8 %	6.3%	1.8%	40.8%	2.5 %
Cyberfraud	65.9 %	3.8 %	6.6 %	11. 8 %	2.1 %	12.4 %	4.1 %	6.8 %
Cyberstalking	66.4%	19.9%	3 %	4.5 %	1.3 %	4.7 %	8.3 %	5.1 %
Wi-Fi Stealing	18.2%	30.7 %	6.8 %	12.8%	30.5 %	21. 9%	4.1 %	13.8%

For the Revenge Porn, the Cyberbullying, the Cyber Fraud and the Cyberstalking case, the most selected option was “it’s not justifiable”. That choice seemed to be consistent with the pattern that has been discussed before in terms of a high self-control sample, and a tendency to rate vignettes as morally unacceptable and not engage in the acts depicted in them. Illegal Downloading, Sexting and Wi-Fi stealing were understood as more justifiable according to the frequencies seen in Table 19.

In relation to the victim of crime (Yes or No) variable, a *chi-square* test demonstrated that in the Illegal Downloading vignette, only the “I didn’t have any other choice” technique showed a distribution of frequencies statistically significant  $p < 0.05$ . The Revenge Porn vignette demonstrated no statistical significance in relation to any of its neutralisation techniques. For the Cyberbullying vignette, no statistical significance was found. In sexting only the “I haven’t done anything wrong” and “everyone else is doing it” were significant at  $p < 0.05$ . In relation to the Cyberfraud vignette, the “I didn’t have any other choice” technique was statistically significant at  $p < 0.05$ . For the Cyberstalking vignette the ledger technique was significant at  $p < 0.05$ , whereas in Wi-Fi Stealing the “it’s not justifiable” narrative was statistically significant at  $p < 0.05$ . There is not enough data to explain why these very specific or particular techniques might be related to the victim of crime variable that has proven to bear no statistical significance in terms of the tests performed with the theoretical construct.

In terms of gender, more *chi-square* tests were run, cross-tabulating every single neutralisation technique. All of the neutralisation techniques that were part of the Illegal Downloading vignette were not statistically significant in terms of gender. Also, the techniques connected to the Revenge Porn, Cyberbullying and Sexting vignettes were not statistically significant either.

In the case of Cyber Fraud, the “It’s not justified”, “I didn’t have any other choice” and “everyone else is doing it” techniques were statistically significant at  $p < 0.05$ . In relation to all the Cyberstalking neutralisation techniques, no statistical significance was found. Finally, in relation to the Wi-Fi stealing case, the “everyone else is doing it” and “It is my right to do so” were significant at  $p < 0.05$ .

In relation to self-control, firstly, the analysis was carried out for the “It’s not justifiable” neutralisation technique, by using a T-Test comparing the self-control means. The “unjustified” technique was used as the grouping variable, dividing the sample between those who thought the vignettes were not justifiable and those who thought it was. The *t-values* were negative: respondents who picked the unjustified technique had lower means of self-control (therefore higher levels of self-control) than those who did not pick it). This is the trend that was going to be repeated in these set of measures with two exceptions (Table 20).

**Table 20. Self-control means by unjustified (Yes or No) and distribution of unjustified amongst self-control groups**

	Self-Control (Unjustifiable: Yes/No)	Self-Control(High/Low)
Illegal Downloading	$t(660) = -5.20^{***}$	$X^2(1, N = 662) = 6.12^*$
Revenge Porn	$t(660) = -3.00^{***}$	$X^2(1, N = 662) = 8.73^{**}$
Cyberbullying	$t(660) = -1.10$	$X^2(1, N = 662) = 1.04$
Sexting	$t(660) = -0.87$	$X^2(1, N = 662) = 0.15$
Cyberfraud	$t(660) = -2.41^*$	$X^2(1, N = 662) = 3.43$
Cyberstalking	$t(660) = -2.21^*$	$X^2(1, N = 662) = 1.83$
Wi-Fi Stealing	$t(660) = -4.34^{***}$	$X^2(1, N = 662) = 2.43$

Legend \*  $p < 0.05$ / \*\*  $p < 0.01$ / \*\*\*  $p < 0.001$



Secondly, *chi-square* tests were used when cross-tabulating the categorical dichotomous variable SelfControl(High/Low) with all the Unjustifiable dummy variables.

By using this procedure, only Illegal Downloading and Revenge Porn were statistically significant (Table 20). It appears that, even though the people who picked the “Unjustifiable” neutralisation technique had higher levels of self-control overall than those who did not. It does not really mean that those who picked this neutralisation tended to have high self-control.

Finally, in order to test all of the respondents who picked the neutralisation technique unjustifiable (instead of performing tests on a case by case scenario), and compare them with the self-control interval variable, a new variable was computed called SUM\_Unjustified. This variable comprised all the cases that had answered the Unjustifiable technique. Each of the eight options from the neutralisation techniques questions were coded into dummy variables (whose data were either 1 for “picked” or 0 for “not picked”). This resulted in 7 (Cases 1-7) different dichotomous variables for the “it’s not justified” script (as well as seven other variables for “Nothing wrong”, plus other seven for “It’s not my fault” and subsequently for all the others. Given the importance of the “it’s not justified” script (as it supposed the absence of neutralisations), the newly computed Sum\_Unjustified categorical variable contained the seven cases’ unjustified variables.

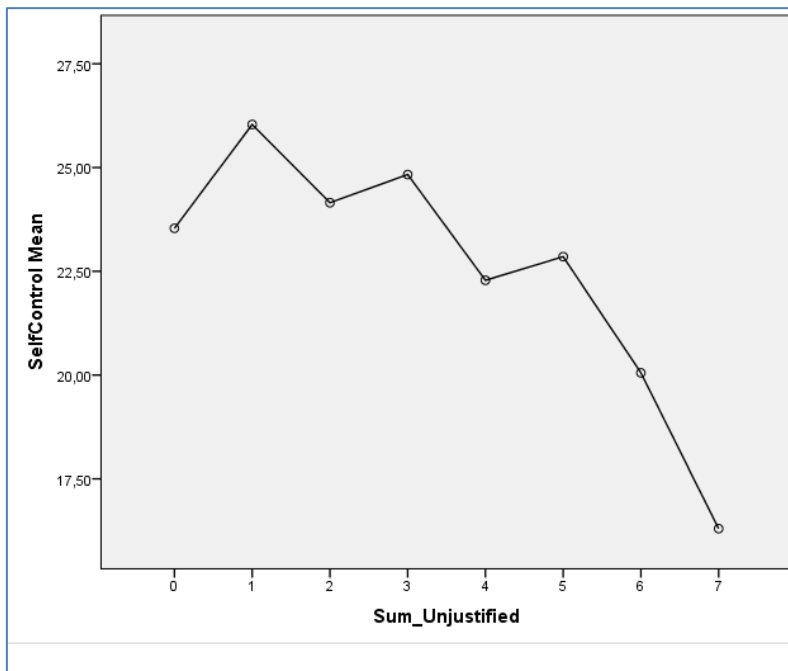
**Table 21. Frequency table for Sum\_Unjustified**

<b>Sum_Unjustified</b>		
	Frequency	Percentage
	0	105
	1	57
	2	63
	3	100
Valid	4	161
	5	130
	6	61
	7	32
Total	709	100,0

The variable ranges from 0 – 7 (Table 21) meaning that 105 respondents (14.8%) did not pick the technique “it’s not justifiable” in any situation, 7 would mean that only 32 respondents (4.5%) picked “it’s not justifiable” in all of the seven cases. The Mode was 4, meaning that 161 respondents (22.7%) had picked “it’s not justifiable” in four cases. Theoretically, individuals that tend to understand most of the cases as unjustifiable would demonstrate higher levels of self-control and ought to demonstrate less crime propensity. Hence, it would be necessary to compare the self-control means of these different 8 groups. An ANOVA was carried out using Sum\_Unjustified as the factor and self-control as the dependent variable. The result was  $F(7, 654) = 4.51, p < 0.001$ . What the result indicated is that participants who had picked “unjustified” more times, tended to have lower means of self-control (higher levels of self-control). The ANOVA results seemed to be congruent with those from the T-Tests. Therefore, it seemed that there was a significant relationship between self-control and the use of a negative neutralisation technique. The necessity of not justifying a criminal action was, therefore, linked with higher levels of self-control. Also, a *chi-square* Test compared the distribution of the 8 “unjustified” groups in the Self\_Control(High/Low) dichotomous variable and resulted in

$\chi^2(7)=15.26$ ,  $p<0.05$ , this seemed to indicate that there were more members of the high self-control group amongst those who picked the “unjustified” justification more times.

**Figure 18. Means plot for self-control and Sum\_Unjustified**



In order to analyse the other seven types of neutralisation technique and their relationship with self-control, T-Tests were performed by using each of the neutralisation techniques as the grouping variables thereby creating two sub-samples in terms of self-control means.

**Table 22. Comparison of self-control means by all neutralisation techniques and distribution of those who picked neutralisations techniques by Self-Control High\_Low (only statistically significant portrayed)**

	Self-control	Self-control High_Low
Illegal Downloading	Not my fault: $t(660)=2.54^*$	-
Revenge Porn	Victim's fault: $t(660)=3.21^{**}$	Nothing wrong: $\chi^2(1, N=662)=6.89^{**}$ Not my fault: $\chi^2(1, N=662)=4.79^*$ Victim's fault: $\chi^2(1, N=662)=9.84^*$
Cyberbullying	Everyone else is doing it: $t(660)=2.22^*$	-
Sexting	Not my fault: $t(660)=3.00^{**}$ No other choice: $t(660)=3.18^{**}$	Not my fault $\chi^2(1, N=662) = 10.37^{**}$ No other choice: $\chi^2(1, N=662)=4.03^*$
Cyberfraud	Nothing wrong: $t(660)=2.97^{**}$ Not my fault: $t(660)=2.80^{**}$ It's my right to do so: $t(660)=2.01^*$	Not my fault : $\chi^2(1, N=662)= 8.06^{**}$
Cyberstalking	Victim's fault: $t(660)=2.73^{**}$	victim's fault (1, N=662) = $8.35^{**}$
Wi-Fi stealing	Not my fault: $t(660)=3.13^{**}$ No other choice: $t(660)=2.32^*$ It's my right to do so: $t(660)=3.12^{**}$	It's my right to do so: $\chi^2(1, N=662)= 6.38^*$

Legend \* $p<0.05$ /\*\*  $p<0.01$

All of the results shown in Table 22 were statistically significant, meaning that only the differences in self-control means were relevant. For example, in Revenge Porn (the highest *t-value*) those who chose "victim's fault" demonstrated lower levels of self-control to those who did not. The same pattern applied to the other techniques. The number of results that have proven to be statistically significant is twelve and only one two or three per case, a very small number taking into account that there were seven techniques per vignette (not counting the "unjustified" technique).

Table 22 also depicted the significant distributions of Self-Control High and Low, amongst those who picked a certain neutralisation techniques and those who did not. The statistically significant distributions showed the groups of High Self\_Control group are usually found among those individuals not picking neutralisation techniques.

In sum, participants who picked neutralisations techniques demonstrated lower levels of self-control. However, the number of neutralisation techniques found significant is small (taking into account that there are seven techniques per vignette, and a total of 49 different choices, without counting the “unjustified” technique). In Table 22, the statistically relevant results that coincided in the interval self-control variable and the dichotomous self-control variable (High\_Low) have been highlighted in darker colour.

In relation to neutralisation techniques, the analysis commenced with T-Tests, comparing the morality means of independent samples using the “unjustified” categorical dichotomous variable as the grouping variable. For Case 1, the “unjustified” variable that was used was Case1\_Unjustified, for Case 2 it was Case2\_Unjustified, and so on. Finally, ANOVAs were also performed with aggregated neutralisation variables. The participants who picked “unjustified” as a neutralisation technique for a given case, demonstrated higher means for the morality variable regarding the case in hand (they rated it as more morally unacceptable than those who did not pick the unjustified technique for the case). This can be seen in Table 23.

**Table 23. Morality means' comparison by “Unjustified” neutralisation technique**

	Unjustified
Illegal Downloading Morality	t(705)=7.22***
Revenge Porn Morality	t(704)=4.87***
Cyberbullying Morality	t(699)=4.36***
Sexting Morality	t(704)=15.05***
Cyberfraud Morality	t(703)=5.86***
Cyberstalking Morality	t(706)=6.70***
Wi-Fi Stealing Morality	t(706)=11.65***

Legend: \*\*\* p<0.001

All of the *t-values* were positive and statistically significant at  $p<0.001$ . The *t-values* were very high, yet much higher for the sexting and Wi-Fi Stealing cases (Table 23). For example, in the Wi-Fi Stealing vignettes the morality means of those who picked unjustified=6.89 and the ones who did not pick unjustified=3.75. Similarly, for the Sexting vignette ( $t(704) = 15.05$ ,  $p<0.001$ ), those who picked unjustified cases showed morality means= 8.42 as opposed who did not pick unjustifiable whose means=4.50. The differences were also notable for the Illegal Downloading vignette, although they were not as dissimilar as in the sexting and Wi-Fi stealing vignettes.

This was consistent with the theorised model and the patterns that have been established in the present study. Respondents who rated a certain case as morally adverse were more likely to understand that very same case as unjustifiable when confronted with the neutralisation question. This is more apparent in the engagement questions as individuals who would not engage in cybercrime case might not feel the hypothetical need to justify it in order to protect themselves from blame. It is very noticeable how people that understood Sexting as

unjustifiable have rated it with a high moral fail, whilst those who did not pick the unjustifiable option rated it with moral neutrality or ambivalence. Sexting was the vignette that generated the most dispersion in terms of moral views and that seemed to be mirrored in this situation.

In all the cases, it seemed that the morality of a case determined the need for not justifying it and using a neutralisation technique. Therefore, there existed a significant relationship between perceptions of morality and the absence of neutralisation techniques.

Finally, ANOVAs were performed using Sum\_Unjustified as the factor and being the dependent variables the perceptions of morality questions. Results are displayed in Table 24.

**Table 24. ANOVAs using Sum\_Unjustified as factor and morality questions as dependent variables**

	ANOVA (Sum_Unjustified)
Illegal Downloading Morality	F (7, 699) =9.99***
Revenge Porn Morality	F (7, 698) =2.47*
Cyberbullying Morality	F (7, 693) =1.75
Sexting Morality	F (7, 698) =13.35***
Cyberfraud Morality	F (7, 697) =3.82***
Cyberstalking Morality	F (7, 700) =4.74***
Wi-Fi Stealing Morality	F (7, 700) =15.43***

Legend: \* p<0.05/ \*\*\*p<0.01

All of these ANOVAs tended to demonstrate that, the more times the “Unjustifiable” variable was picked, the perceptions of morality of a scenario became more and more unacceptable. Usually, respondents who had picked the unjustified neutralisation technique in all seven vignettes demonstrated the higher means in the perceptions of morality (rated the vignettes with moral fail). The highest F ratios were found in Sexting and Wi-Fi Stealing (Table 24), being

those the cases were the mean difference became much more apparent between respondents that hadn't picked unjustified in any case and those who have in some or all cases. The only non-statistically significant case in terms of ANOVA was the cyberbullying case (even though in this case, the morality means also tended to increase in the groups that have picked unjustifiable more times).

In relation to the other seven neutralisation techniques, T-Tests were performed by using each of the neutralisation techniques (applying to each vignette only the neutralisations coded for that vignette) as the grouping variables for the creation of two sub-samples of morality means. The T-Test showed results that are extremely relevant to the theoretical model. The significant neutralisation techniques had negative *t-values*, therefore those respondents who had picked one of them (the ones that have been deemed as statistically significant) showed lower means of morality. Neutralisation techniques allowed participants to see cybercrimes in a more acceptable way in terms of its immorality, therefore fulfilling one of the key purposes of neutralisation techniques, which is protecting oneself from blame and the blame of others by resorting to conventional views of morality.



**Table 25. Comparison of morality means by all neutralisation techniques (only statistically significant portrayed)**

	Neutralisations
<b>Illegal Downloading Morality</b>	Nothing wrong: $t(705)=-7.92^{***}$ Not my fault: $t(705)=2.45^*$ Everyone else is doing it: $t(705)=2.28^*$ It's my right to do so: $t(705)=-4.99^{***}$
<b>Revenge Porn Morality</b>	Victim's fault: $t(704)=-2.62^{**}$ It's my right to do so: $t(704)=-3.76^{***}$ Everyone else is doing it: $t(704)=-3.26^{**}$
<b>Cyberbullying Morality</b>	Nothing wrong: $t(699)=-2.06^*$ Victim's fault: $t(699)=-2.40^*$ Not my fault: $t(699)=-4.14^{***}$ No other choice: $t(699)=-2.70^{**}$ It's my right to do so: $t(699)=-3.41^{**}$
<b>Sexting Morality</b>	Nothing wrong: $t(704)=-8.96^{***}$ It's my right to do so: $t(704)=-5.69^{***}$
<b>Cyberfraud Morality</b>	Nothing wrong: $t(703)=-6.28^{***}$ Not my fault: $t(703)=-4.14^{***}$ It's my right to do so: $t(703)=-6.70^{***}$ Victim's fault: $t(703)=-2.08^*$ Everyone else is doing it: $t(703)=-2.22^*$
<b>Cyberstalking Morality</b>	Nothing wrong: $t(706)=-3.95^{***}$ Not my fault: $t(706)=-3.64^{***}$ Victim's fault: $t(706)=-2.89^{**}$ It's my right to do so: $t(706)=-4.05^{***}$
<b>Wi-Fi Stealing Morality</b>	Nothing wrong: $t(706)=-10.05^{***}$ Victim's fault: $t(706)=-2.53^*$ It's my right to do so: $t(706)=-4.20^{***}$

Legend \* $p<0.05$ /\*\*  $p<0.01$ /p \*\*\*  $<0.001$

In Table 25, the first technique that was statistically significant was “nothing wrong” ( $t(705) = -7.92$ ,  $p<0.001$ ). In this case the mean difference was very high and participants who used this technique rated illegal downloading  $M=1.87$  ( $n=150$ ), therefore understanding it as almost not immoral at all. By contrast, those who did not pick the technique had a mean of 3.81 ( $n=557$ ). Something similar occurred with “It's my right” ( $t(705) = -4.99$ ,  $p<0.001$ ).

However, an opposite trend emerged for “not my fault”  $p < 0.05$  and “everyone else is doing it”  $p < 0.05$ . In these cases, *t-values* were positive, and those who picked the technique rated illegal downloading as more morally inadequate.

Nothing wrong seemed to be the most effective technique in terms of shielding against morality, with very high *t-values* and statistically significant in every vignette in relation to morality; with the exception of Revenge Porn vignette.

In relation to the engagement variables and neutralisation variables, the analyses were carried out in the same way as for the morality variables, employing T-Tests and ANOVAs. The T-Tests used the “Unjustified” variables as the grouping variable in order to compare the means of engagement (Following this sequence of comparisons: Case1\_Unjustified for Vignette number 1, Case2\_Unjustified for vignette number 2, etc.). All of the *t-values* were negative and statistically significant at  $p < 0.001$ , with the exception of Cyberstalking that was significant at  $p < 0.05$ .

**Table 26. Engagement means' comparison by Unjustified neutralisation techniques.**

	Unjustified
Illegal Downloading Engagement	t(705)= -3.99***
Revenge Porn Engagement	t(702)= -5.97***
Cyberbullying Engagement	t(705)= -7.01***
Sexting Engagement	t(703)= -5.06***
Cyberfraud Engagement	t(704)= -5.98***
Cyberstalking Engagement	t(704)= -2.20*
Wi-Fi Stealing Engagement	t(707)= -10.342***

Legend: \*p<0.05/ \*\*\* p<0.001

For every single case, the engagement means of respondents who picked the “it’s not justifiable” option were lower than those who had not picked this option. This difference, as indicated beforehand, was statistically significant for every single case (see Table 26).

The *t-value* for Wi-Fi Stealing vignette (t(707) =-10.342, p<0.001) was the highest one and demonstrated a very profound difference in the means. This might indicate that participants who did not understand Wi-Fi Stealing as unjustifiable would almost certainly engage in it (a score of 10 demonstrates absolute agreement). All of this is consistent with the theoretical model and demonstrated congruency between the engagement variables and the neutralisation techniques.

The ANOVAs were performed using Sum\_Unjustified as the factor and the engagement questions as the dependent variables (see Table 27).

**Table 27. ANOVAs using Sum\_Unjustified as factor and engagement questions as dependent variables**

	ANOVA (Sum_Unjustified)
Illegal Downloading Engagement	F (7, 699) =4.27***
Revenge Porn Engagement	F (7, 696) =4.17***
Cyberbullying Engagement	F (7, 699) =2.64*
Sexting Engagement	F (7, 697) =1.81
Cyber Fraud Engagement	F (7, 698) =2.80**
Cyber Stalking Engagement	F (7, 698) =0.53
Wi-Fi stealing Engagement	F (7, 701) =15.12***

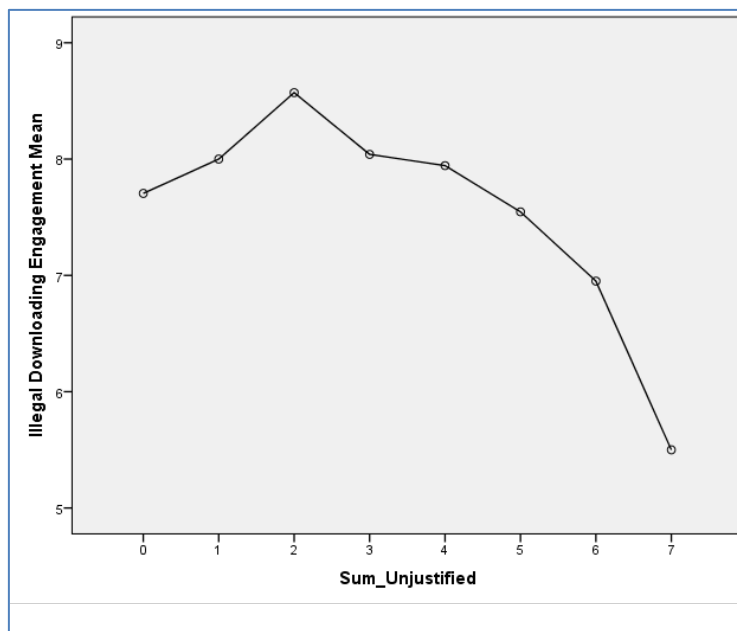
Legend: \* p<0.05/\*\* p<0.01/ \*\*\*p<0.001

All of the cases were statistically significant, with the exception of sexting and cyberstalking.

The trend is that respondents who more frequently chose the option “it’s not justifiable” were less likely to engage in acts of cybercrime, given that their engagements means were lower.

Figure 19 is an example of what has been indicated before.

**Figure 19. Means plot for Illegal Downloading Engagement and Sum\_Unjustified**



All in all, the engagement variables were also statistically significant, in general terms, in relation to the use of a null neutralisation technique.

In relation to the other seven neutralisation techniques, the analysis that was carried out by using T-Tests to compare the engagement means and the different neutralisation technique dummy variables as grouping variables (as seen before, on a vignette by vignette scenario). That analysis (see Table 28) demonstrated that participants who picked a neutralisation technique are more likely to engage in the cybercriminal acts depicted in the vignettes because they show higher engagement means. In these cases, the *t-values* were positive (as opposed to the trend set for the morality values). This became relevant in relation to the theoretical model, as neutralisation techniques serve a twofold purpose. Neutralisation techniques shield against the moral wrongness of the act and accordingly they give the participant more reasons to engage in acts of crime. These tests have therefore proven to be congruent with literature on neutralisation techniques. It is worth mentioning that “nothing wrong” was one of the most

efficient neutralisation techniques, as it has demonstrated very profound differences in the means of some cases and seemed to be favoured by the respondents in general. After analysing the role of neutralisation techniques in perceptions of morality and engagement, one could argue that “nothing wrong” served as the generic neutralisation technique, which allowed for a more abstract modulation of blame. On the other hand, “victim’s fault” was extremely efficient in crimes that have an apparent victim (like those relating to abuse), even in terms of property crime (Wi-Fi Stealing and Illegal Downloading). Even though there were some differences in the techniques that can modulate morality and the ones that can modulate engagement.

Finally, it be pointed out that “I didn’t have any other choice” and “It’s my right to do so” have shown statistical significance in relation to many of the scenarios. “No other choice” was extremely recurrent for the engagement variable (being significant in six of the seven scenarios as can be seen in Table 28).

**Table 28. Comparison of engagement means by all neutralisation techniques (only statistically significant portrayed).**

	Neutralisations
Illegal Downloading Engagement	Nothing wrong: $t(705)=2.87^{**}$ Victim's fault: $t(705)=2.51^*$ No other choice: $t(705)=2.08^*$
Revenge Porn Engagement	Nothing wrong: $t(702)=3.06^{**}$ Victim's fault: $t(702)=4.14^{***}$ Everyone else is doing it: $t(702)=2.94^{**}$ No other choice: $t(702)=3.33^{**}$
Cyberbullying Engagement	Nothing wrong: $t(705)=3.48^{**}$ Not my fault: $t(705)=4.04^{***}$ Victim's fault: $t(705)=2.34^*$ Everyone else is doing it: $t(705)=2.32^*$ No other choice: $t(705)=4.58^{***}$ It's my right to do so: $t(705)=5.74^{***}$ Ledger: $t(705)=2.12^*$
Sexting Engagement	Nothing wrong: $t(703)=3.99^{***}$ No other choice: $t(703)=2.47^*$ It's my right to do so: $t(703)=3.17^{**}$
Cyber Fraud Engagement	Nothing wrong: $t(704)=4.29^{***}$ Not my fault: $t(704)=3.93^{***}$ Everyone else is doing it: $t(704)=2.14^*$ No other choice: $t(704)=3.00^{**}$ It's my right to do so: $t(704)=3.05^{**}$ Ledger: $t(704)=2.10^*$
Cyber stalking Engagement	Victim's fault: $t(704)=2.36^*$ It's my right to do so: $t(704)=3.03^{**}$
Wi-Fi Stealing Engagement	Nothing wrong: $t(707)=6.30^{***}$ Victim's fault: $t(707)=2.58^*$ Everyone else is doing it: $t(707)=2.71^{**}$ No other choice: $t(707)=4.64^{***}$ Ledger: $t(707)=2.24^*$

Legend \* $p<0.05$ /\*\*  $p<0.01$ /p \*\*\*  $<0.001$

Several problems must be mentioned in relation to the T-Tests that were used in Revenge Porn. The independent samples compared for “nothing wrong” and “everyone else is doing it”, were very imbalanced (for “nothing wrong” ( $n_1=10$ ,  $n_2=694$ ) and for “everyone else is doing it” ( $n_1=3$ ,  $n_2=701$ )). In cyberbullying the same occurred with “no other choice” ( $n_1=5$ ,  $n_2=702$ ). In Sexting, “no other choice” was significant at  $p<0.05$  with a positive t-value and an unbalanced sample ( $n_1=13$ ,  $n_2=392$ ).

Cyberbullying was the vignette that had the most significant neutralisation techniques in terms of engagement. This is relevant in social terms and crime prevention terms, but it could also provide a discourse educationally and how cyberbullying is understood by the sample as a justifiable process. Contrarily, the means of engagement and morality seemed to indicate that cyberbullying was seen as repulsive by the sample, maybe needing more neutralisations in order to become palatable.

Table 29 is a summary of all the statistically significant neutralisation techniques discussed in this chapter. Columns indicate whether they were significant in relation to the morality variable, the self-control variable or the engagement variable. The ones that were statistically significant in relation to the three variables have been coloured in order to highlight their efficiency and intensity. Also, the cyberbullying engagement cell has been highlighted in dark colour in order to show that it is the only case where the seven neutralisations were effective.



**Table 29. Statistically significant neutralisation techniques in relation to self-control, morality and engagement**

	Self-control (interval and dichotomous variables)	Morality	Engagement
Illegal Downloading	-	Nothing wrong	Nothing wrong
	Not my fault	Not my fault	-
	-	-	Victim's fault
	-	Everyone else is doing it	-
	-	-	No other choice
	-	It's my right to do so	-
	-	-	-
Revenge Porn	Nothing wrong	-	Nothing wrong
	Not my fault	-	-
	Victim's fault	Victim's fault	Victim's fault
	-	Everyone else is doing it	Everyone else is doing it
	-	-	No other choice
	-	It's my right to do so	-
	-	-	-
Cyberbullying	-	Nothing wrong	Nothing wrong
	-	Not my fault	Not my fault
	-	Victim's fault	Victim's fault
	Everyone else is doing it	-	Everyone else is doing it
	-	No other choice	No other choice
	-	It's my right to do so	It's my right to do so
	-	-	Ledger
Sexting	-	Nothing wrong	Nothing wrong
	Not my fault	-	-
	-	-	-
	-	-	-
	No other choice	-	No other choice
	-	It's my right to do so	It's my right to do so
	-	-	-
Cyber Fraud	Nothing wrong	Nothing wrong	Nothing wrong
	Not my fault	Not my fault	Not my fault
	-	Victim's fault	-
	-	everyone else is doing it	Everyone else is doing it
	-	-	No other choice
	It's my right to do so	It's my right to do so	It's my right to do so
	-	-	Ledger
Cyber stalking	-	Nothing wrong	-
	-	Not my fault	-
	Victim's fault	Victim's fault	Victim's fault
	-	-	-
	-	-	-
	-	It's my right to do so	It's my right to do so
	-	-	-
Wi-Fi stealing	-	Nothing wrong	Nothing wrong
	Not my fault	-	-
	-	Victim's fault	Victim's fault
	-	-	Everyone else is doing it
	No other choice	-	No other choice
	It's my right to do so	It's my right to do so	-
	-	-	Ledger

#### 4.3.4. Regression

Finally, in order to test the strength of some elements of the model, a regression was carried out. A linear regression using the stepwise method that tried to predict the interval self-control aggregated value (dependent variable) by using all morality and engagement questions as predictor variables.

Step 7 ( $R^2 = 0.198$ ,  $F(7, 635) = 22.836$ ,  $p = 0.000$ ), including the variables listed below, predicted a significant variance in self-control scores:

- Revenge Porn Engagement:  $\beta = 0.187$ ,  $t = 5.130$ ,  $p = 0.000$
- Cyber Fraud morality:  $\beta = -0.225$ ,  $t = -5.740$ ,  $p = 0.000$
- Wi-Fi stealing engagement:  $\beta = 0.141$ ,  $t = 3.454$ ,  $p = 0.001$
- Illegal Downloading Engagement:  $\beta = 0.122$ ,  $t = 2.936$ ,  $p = 0.003$
- Cyberfraud engagement:  $\beta = 0.095$ ,  $t = 2.478$ ,  $p = 0.013$
- Illegal Downloading morality:  $\beta = -0.102$ ,  $t = -2.625$ ,  $p = 0.009$
- Sexting morality:  $\beta = 0.097$ ,  $t = 2.583$ ,  $p = 0.010$

All of these variables significantly predicted self-control, even though some were negative values, such as Illegal Downloading morality and Cyberfraud morality. This can be understood from the perspective that an increase in the morality variables (the higher the perception of moral wrongness) would suppose a decrease in self-control scores. The more morally wrong any of these acts is perceived, the higher the degree of self-control respondents have. By contrast, engagement variables had positive  $\beta$  values, therefore increases in any of them would suppose an increase in the self-control interval variable. In other words, the more likely a person is to engage in acts of crime, the less self-control they would have.

Results were consistent with what has been indicated in the previous regression and throughout this chapter.

## **4.4. Discussion**

Even though the presentations of findings originated some immediate discussion, this part of the chapter is dedicated to analyzing certain specific issues in more depth, bearing in mind that the final chapter of this work contains an integrated discussion of both the quantitative and the qualitative results.

### **4.4.1. Morality**

The worst rated vignette, deemed to be almost absolutely immoral, was the Revenge Porn vignette, followed by the Cyberbullying vignette. They correlated positively very strongly. Two things must be discussed in relation to this: first, whether or not Revenge Porn and Cyberbullying are understood taxonomically as two different criminal species or Revenge Porn as a subspecies of Cyberbullying; and secondly, whether or not the sexual (be it erotic or pornographic) nature of Revenge Porn has been ascribed more intense immoral connotations. The Revenge Porn case has been phrased by the present researcher as researcher as:

“Peter and Adele were going out. Adele used to send Peter suggestive pictures of her accompanied by saucy messages. One day Peter discovers Susan is having an affair and he decides to take revenge on her by sending her pictures and messages to his friends via social networks and e-mail, as well as posting them on the internet<sup>x</sup>. “

A gender discourse might be of interest in order to understand better this vignette. It could be argued that patriarchal structures inform the idea of a man taking revenge on a woman by using her own sexuality as a weapon of shame. This issue will be dealt with in more detail in Chapter 6. However, a T-Test demonstrated that women ( $n=398$ ,  $M=9.42$ ) rated this vignette morally worse than men ( $n=308$ ,  $M=8.92$ ),  $t(704) = -3.50$ ,  $p < 0.001$ . Going back to the four “precipice” vignettes (Cyberbullying, Cyberstalking, Cyberfraud and Revenge Porn), these were the cases that have shown the strongest correlations between their morality variables as indicated in previous paragraphs. One could argue these were the most extreme situations; ones that imply a certain level degree of cruelty or a harassing attitude. These four vignettes also imply psychological violence and could be understood as extremely destructive for the victims, given the impact they can have upon them. Cyberfraud may be more diffuse in terms of its psychological impact, but the sample may have perceived it as having a profound victimising impact. In addition, all these behaviours are criminalised in the Criminal Code in Spain. (In some cases, like Revenge Porn and Cyberstalking, this was not expressly so until July 1<sup>st</sup> 2015 when the criminal Code was amended). Therefore, codified crime (rather than deviant behaviour or administrative wrongs) might be regarded as inherently morally wrong by a sample with high self-control (that include low levels of egotism). Also, it must be taken into account that the sample was comprised mostly of university students (including criminology and law students), law enforcement agents, educators and lawyers. In conclusion, most of the respondents had an understanding of crime from an ontological and philosophical perspective that allowed them to ascribe negative moral labels to different situations that are understood as criminal.

In the Sexting vignette a gender discourse might also shed some light, given that the question was formulated in the following manner:

“Gena is a 16 year old young girl that thanks to a social network has befriended a 31 year old man called Bad\_Wolf and started a relationship of sexual undertones. One day Bad\_Wolf asks Gena to send some naked pictures of her, she agrees and does it”<sup>xi</sup>.

In this case, the gender of the main character was deliberate in order to study whether gender played a fundamental part in moral rating, from the point of view of the ones rating or the one being rated. Following a T-Test, comparing women (n=399, M=5.64) and men (n=307, M=5.34), no statistical significance ( $t(704) = -1.116, p > 0.05$ ) was found in the comparison of means between males and females rating the morality of the sexting case. This case created several divisions in terms of perceptions of morality, but said opinions seemed not to rely on the gender of the participants. The reasons why both men and women tended to rate the Sexting and Cyberstalking vignettes similarly raised several gender issues that should be dealt with. Men and women positioned themselves in “lukewarm morality” in relation to the Sexting vignette. In addition to this, both men and women rated Cyberstalking with a very high “moral fail” (men, n=308, M=8.71; women, n=400, M=8.76). The Cyberstalking vignette was depicted as follows:

“Tom is secretly in love with his work-mate Deborah. On a daily basis he sends her love e-mails from a fake e-mail account signed as ‘Your secret admirer’. Tom has also created a web-page called ‘DeborahIwouldDevourYou.com’ where he posts pictures of her taken without permission and love letters. Deborah feels very worried and scared about this”<sup>xii</sup>.

The narrative portrayed an innocent female victim, falling victim to obsessive predatory behaviour from a male colleague. Both male and female participants rated this case very similarly, where they have rated other cases (in terms of morality) in a differently. Revenge Porn that included a similar situation, whereby a man shares intimate sexual content, to take

revenge on his girlfriend, was deemed to be much more wrong ( $t(704) = -3.50, p < 0.001$ ) by women. Also, another similar abusive situation like Cyberbullying showed significant differences between sexes. On a statistical level, the Revenge Porn vignette and the Cyberstalking one were positively correlated at  $r = 0.55$ .

One could argue that a chivalry explanation might be behind these differences (men constructing women as “damsels in distress”), or a feminist discourse (women being more empathic towards abused women) or a combination of both (Juschka, 2009). These issues will be brought up again in Chapter 6, when integrating data from the online survey and the interviews. The differences in the vignette scores might also lie in the fact that in Revenge Porn, no indication of the psychological state of the victim was made, whereas in the Cyberstalking vignette the coda “Deborah feels very worried and scared about this” was provided. Even so, the Revenge Porn vignette obtained higher ratings from both sexes than the cyberstalking one. This is also the first case where the participants were asked to rate the victim instead of the perpetrator in order to see whether or not morality and engagement would differ from other vignettes. Also, the perpetrator was named *Bad\_Wolf* to accentuate the sense of menace or threat.

It should be recognized that the victim, Gena, in the Sexting scenario, was a 16 year old girl (a minor in Spain) who was convinced by an adult to send naked pictures of herself in what seemed to be a consenting relationship. This should have no apparent legal repercussions, even though a good knowledge of law would be needed to understand the particularities of the case. In other words, the idea was creating a vignette that was to be rated from a non-legalistic point (not as a crime) of view but a purely moral perspective.

It might be argued that these cases are not understood as immoral, because they are not regarded as crimes by the sample (albeit illegal downloading is a crime against intellectual property in Spain, as an example). This is a study on perceptions of morality and as such there is a focus upon participant's construction of the world. Illegal Downloading has become part of many people's daily lives, a habit. Also, neutralisation techniques operate in order to protect the offender from blame relating, for example, from the music industry. Something similar occurred in relation to Wi-Fi Stealing, as it is understood as a normalized pattern of behaviour.

As a summary, the majority of vignettes have been perceived as morally repulsive by participants with the exceptions of Sexting ("lukewarm"), Wi-Fi Stealing and Illegal Downloading (both acceptable). Also, self-control in itself has proven to be statistically significant as those with higher levels of self-control rated the cases as less morally acceptable. Women have demonstrated higher levels of self-control and higher means in the perceptions of morality in general.

#### **4.4.2. Engagement**

In terms of engagement, participants generally demonstrated low tendencies to engage in the activities depicted, with the exception of Illegal Downloading and Wi-Fi stealing. This, if considered with the morality results, demonstrated that the sample had very low cybercrime propensity.

Engagement being statistically significant in terms of self-control was consistent with the proposed theoretical model and with the overall pattern of results. Individuals with high levels of self-control (those with lesser scores in the Grasmick scale) are socio-psychologically fit to avoid and postpone immediate pleasure and have stronger cognitive instruments to deal with frustration. They are, therefore, not likely to engage in acts of crime. Lack of self-control does not only mean being impulsive, but also to have a here and now mentality with the inability to position oneself in the future, the inability to position oneself in the place of others, the dislike for complex tasks, the need for taking risks, a liking for physical activities (rather than mental ones) and the inability to reason verbally in conflicts (Gottfredson & Hirschi, 1990). As Higgins (2001) stated “the lower an individual’s level of self-control, the more likely they are to perform digital piracy and to highly value digital media” (p.148). Higgins also found correlations between shame, value, external sanctions, moral behaviors and low self-control with digital piracy (pp. 147-148).

The present study also seemed to indicate that individuals with higher levels of self-control would rate cybercrimes as more morally repulsive than those with lesser levels of self-control. A high self-control sample like the one in this study shows, in summary, less propensity to the commission of cybercrimes.

One case that stands out is the Sexting vignette. Contrary to what has been theorized and demonstrated in terms of correlations and measures of engagement and morality, participants understood Sexting as not entirely right or not entirely wrong. That being the case, it could be argued that participants would not mind engaging in Sexting. However, the sample was not keen on performing sexting (in a similar fashion to the other vignettes, with the exception of Illegal Downloading and Wi-Fi Stealing). Similarly, all of the vignettes were significant in terms



of the relationship between engagement and self-control, but not all of the vignettes were significant in terms of the relationship between perceptions of morality and self-control (Sexting and Illegal Downloading are not).

The answer to this conundrum might be found in the fact that questions ask about eventual involvement in criminal (or pseudo-criminal) activities and, even though, indirect projective questioning was approached by using vignettes, asking the participants to “put themselves in some else’s shoes” (used for neutralisation techniques) and whether they “would do the same someone did on the vignette” in order to avoid becoming a self-report questionnaire. Fisher (1993) reviewed several studies based on indirect projective questions, such as the ones found in this study but with no criminological undertones. According to Fisher (1993) “The stronger the social norms governing the topic under investigation, the more likely social desirability bias is to occur” (p. 313). However, Fisher also added “it appears that indirect questions can be constructed that are not significantly affected by social desirability bias” (p. 313). Therefore, asking about the perceptions of morality of actions that are mostly illegal could produce a social desirability bias. Respondents might indicate that they would surely not engage in cybercriminal activities. Similarly, Schoepfer and Piquero (2006) used vignettes to measure moral beliefs and self-control and carried out a vignette based study that served as inspiration for the methodology of this investigation. They indicated that “Although we readily acknowledge that the use of hypothetical circumstances is not necessarily equivalent to reality; previous research has revealed a strong correlation between intentions and actual behavior” (Schoepfer & Piquero, 2006, p. 58; citing, Green 1989; Kim, and Hunter 1993; Pogarsky 2004; see also Wikström et al., 2003). After acknowledging the limitations of their study, Schoepfer and Piquero (2006) stated that “future research should strive to replicate our results using actual behavior” (p. 68). In a similar fashion, Randall and Fernandes (1991) also

researched social desirability bias and concluded that “ethical individuals provide socially desirable responses that agree with their behavior” (p. 813) and that “our research demonstrated that social desirability bias persists even if the survey is administered in a non-threatening situation” (p. 813). In accordance, a high self-control sample obtained mostly from university students, lecturers, lawyers or police officers might tend to demonstrate ethical behavior reflected on the scores (by rating the vignettes as morally unacceptable and not engaging in them). However, the fact that most of the data was collected by using an online questionnaire that guaranteed real anonymity might have minimized the impact of the bias in the responses.

From another perspective, one could argue that some of the differences found between the morality and the engagement questions might be understood because of the existence of the “fundamental attribution error” or “correspondence bias”, “the correspondence bias is sometimes denned as the tendency to underestimate the power of situations” (Gilbert & Malone, 1995, p. 27). The reason why the aforementioned bias might occur in this study could be grounded in the idea that morality questions might be understood as the ascription of a certain general moral makeup to others. The participant, when indicating the moral appropriateness of sexting (or any of the other depicted behaviours), was judging the “other” or the “average guy”, an abstraction of what he/she understood as the generality of the population. It would entail the creation of an idea akin to the “weak abstract other” as opposed to the “strong-willed I”:

Ordinary people seem to believe that others behave as they do because of the kinds of others they are and because of the kinds of situations in which their behaviors unfold; thus, when a person makes an attribution about another, she or he attempts to determine which of these factors— the other person or the other person's situation—

played the more significant role in shaping the other person's behavior. (Gilbert & Malone, 1995, p. 22)

In the Sexting vignette, for example, participants were asked to rate the morality of actions carried out by an adolescent girl during the course of an online romantic/sexual relationship. A consensus was not reached as participants rated it in very different ways (it must be taken into account again that for the case the mode=10, yet  $M=5.1$  and  $S.D.=3.47$ ). However, participants were not inclined to take part in these activities when they were asked about themselves (For this case, morality and engagement correlate negatively  $r=-0.22$ ,  $p<0.001$ ). In other words, an intersubjective narrative seemed to unravel: even if it seems appropriate, ambivalent or repulsive that a seventeen year old girl engages in sexting, it is not something I myself would be willing to do.

#### **4.4.3. Neutralisations**

The gender or victimhood variable played no role in the picking and using of neutralisation techniques. Also, self-control is statistically significant in relation to the picking of the “it’s not justified” technique. Respondents with higher levels of self-control tended to opt for it and the more they picked the technique, through the survey, the higher their self-control levels. In terms of other neutralisation techniques, a few have demonstrated statistical significance in relation to the self-control means and also to the distribution of high self-control amongst different techniques but no pattern can be identified. Some of the techniques that were statistically significant for both self-control variables were “victim’s fault”, “not my fault”, “It is my right to do so” and “no other choice”.

Morality and engagement variables have proven to be statistically significant in terms of the picking of “unjustified”, but also in relation to other neutralisation techniques that might be chosen and served to facilitate engagement and modest perceptions of morality.

For example, in one of the essential “outlier cases” - Illegal Downloading - only 17.3 % of respondents defined this behavior as Unjustifiable. In contrast, 34.4% of participants justified the act by indicting that “everyone else is doing it”, which is consistent with current literature on the matter, followed by “I haven’t done anything wrong” (21.4%) and “It’s my right to do so” (11.6 %). Ingram and Hinduja (2008), for example, report:

The results indicated that greater acceptance of the techniques associated with denial of responsibility, denial of injury, denial of victim, and appeals to higher loyalty were significant predictors of moderate levels of piracy participation (e.g., downloading 1011,000 MP3s). (p. 356)

Hinduja (2007) stated that:

Denial of Injury, Appeal to Higher Loyalties, Denial of Negative Intent, and Claim of Relative Acceptability were the only techniques significantly related to having pirated software at least once. These four techniques, then, have the ability to release individuals from the tethers of conventional behavior (i.e., respecting intellectual property) and open up the possibility of pirating software should conducive social or situational factors present themselves to encourage the activity. (p. 196)

Hinduja (2007), and Ingram and Hinduja (2008) proved that that neutralisation techniques played a fundamental part in allowing law-abiding individuals to evade moral norms and commit acts of crime (Illegal Downloading) , provided that there is an opportunity for doing so. What has been said about individuals downloading music (law-abiding but opportunistic) is also consistent with the conceptualisation of criminals (and cybercriminals) as individuals with a “limited rationality”, whose criminal acts are precipitated by situational factors (Clarke, 1999; Cornish & Clarke, 1986, 1987; Miró Llinares, 2011; Newman & Clarke, 2003; Yar, 2005).

In terms of engagement, the only vignette where the seven justification techniques were significant in relation to the engagement variable was Cyberbullying, and the only techniques that were statistically significant in terms of morality, engagement and self-control were “victim’s fault”, “not my fault”, “nothing wrong” and “it’s my right to do so”. “Nothing wrong” was by far the most effective neutralisation technique relating to the highest mean differences of perceptions of morality in sexting, illegal downloading and Wi-Fi stealing and the highest mean differences in Wi-Fi Stealing engagement.

#### **4.5. Summary**

The relationship between self-control, perceptions of morality and engagement have been examined to test the new proposed theoretical model; one based upon an interactive process between cybercrime propensity (perceptions of morality and cybercrime engagement), the exposure to a criminogenic setting (as the internet has been theorised to be) and the application of neutralisation techniques.

The sample tended to comprise individuals with high self-control, fairly balanced in terms of gender, but derived largely from a university population. The lack of probabilistic sampling could have generated a socio-demographic imbalance that might account for some moral bias in the results owing to occupational values and cultures.

Having been a victim of crime did not have any effect on the model. It might have been thought that people who had been victims of crime might have had a harsher view on cybercrime. The results, however, pointed in the other direction. On the other hand, gender played a significant role in the model, with women tending to show higher levels of self-control (more membership of the High self-control groups) than men. Also, women rated cybercrime as more morally reproachable and they were less likely to engage in acts of crime. This finding provides a link between self-control, and the perceptions of morality and engagement in the sample. By contrast, gender seemed to bear no significance in terms of neutralisation techniques.

Self-control played a fundamental role in the construct, be it as an aggregated interval scale, a dichotomous (High/Low variable) and in its six constituent elements. However, when all of the constituent elements of self-control were analysed, physical activities bore no significance in the overall construct; there did not seem to be a modulation of morality perceptions or engagement according to this variable. However, self-control was significantly related to perceptions of morality and engagement, as generally those with higher levels of self-control would not engage in certain acts of crime and rated them as morally repulsive. Participants who were members of the High self-control group showed a similar tendency.

When studying perceptions of morality and engagement, the model revealed a high degree of correlation between the two measures. Generally, participants exhibited considerable consensus between rating cases as morally wrong and indicating that they would not engage in them. The fact that some of the depicted cases were crimes might have generated a strong sense of repulsion. Even so, the existence of a social desirability bias and correspondence bias cannot be overlooked, as the instrument was based on indirect, projective questioning. That said, three vignettes stood out in regards to the “symmetry” between morality and engagement and are in deserving of further analysis: the Sexting, the Wi-Fi Stealing and Illegal Downloading vignettes. Wi-Fi stealing and Illegal Downloading were not really perceived as wrong and seemed to be embedded in the daily activities of the respondents. On the other hand, Sexting was not really understood as morally wrong or right. Also, some of the vignettes might have generated psychological triggers relating to empathy because of the wording or the presentation of the case (i.e. Cyberstalking and Sexting) and call also for a gendered analysis. In addition, a regression demonstrated that some of the engagement and morality variables from certain vignettes had predictive value over the self-control variable.

Finally, it has not been possible to determine the role of self-control in terms of neutralisation techniques. It may be that perception of a criminal behaviour as “Unjustifiable” is not related to an individual’s level of self-control. This might suppose a change in the initial formulation of the SAT-RI model. On the other hand, the data pointed to a relationship between neutralisation techniques, and perceptions of morality and engagement. Usually, participants might not engage in acts they understood as unjustifiable and might rate such acts as morally reproachable. In addition, certain specific neutralisation techniques (depending on the vignettes) might serve to dulcify the moral perceptions of an act and/or to allow for engagement. The narratives that allowed for the understanding of the act as non-criminal and

the ones that blame the victim have proven to be extremely efficient in modulating individuals' propensity towards cybercriminal acts.



## **Chapter 5: Findings - Interviews with Law Enforcement Agents**

The findings that emerged from the interviews with law enforcement agents are divided in: offender morality, neutralisation techniques, and police culture. In order to preserve anonymity and confidentiality, references to law enforcement agents (from now on) are made by using their pseudonyms and the pronoun “he” (regardless of their gender). See Annex 4 for a summary of the cases.

### **5.1. Offender Morality**

#### **5.1.1. The professional**

In relation to the construction of the cybercriminal from the point of view of law enforcement agents, one of the narratives that repeated itself through all the interviews was the idea of the “career criminal”. A very high degree of professionalisation was ascribed to cybercriminals by all interviewees. This narrative appeared in cases C1, C3, C10, C11, C13 and C14. It should be noted that all of these cases (with the exception of C1) were cyberfrauds, as they had an economic purpose and satisfied the legal definition of fraud in many criminal codes or legislation. In other cases, the narratives referred to hackers or skilled computer virus designers, although an economic motivation was always present.

Well, what is clear is that they are professionals and they make their living out of that; I mean they do not have other activity no, I mean, this is a complement to... No. No, this is their way of living. (GCEX, C3<sup>xiii</sup>)

The first quality ascribed to these cybercriminals was computer-prowess. The cybercriminal trade requires very high technical competency in order to, for example, design complex viruses, make contingency plans<sup>19</sup>, create bogus web-pages or to navigate through the dark or deep web:

I mean, this is their way of living; you have let's say **good skills**, you speak perfectly, in this case they spoke three or four languages from Russian, English, Spanish, French, ok? I mean, they Eastern European people have a knack for languages. So they have **an incredible gift for learning**, but at the end it is nothing else but a way of living. (GCEX, C3<sup>xiv</sup>)

The minor had **very high computer skills**, he is very timid, he lives in a very small village in Asturias where what is there are cows. (NPEX2, C17<sup>xv</sup>, emphasis added)

Another quality that was ascribed to these “professional” cybercriminals was entrepreneurship. The majority of them were people born in countries where, according to the interviewee accounts, living conditions were more challenging in economic, legal or social terms, compared to Spain. Against this backdrop, a life of crime seemed to be one easy and logical solution, as well as one of the few life-choices available to them. This is worth mentioning as a high degree of empathy (or at least, understanding) seemed to be present among many of the interviewees.

If in your home country you lived in a certain way and you have acquired this knowledge with what...When you arrive in here and putting this knowledge to work you are capable of having a fast and high economic compensation, having a standard of living you

---

<sup>19</sup> They had several back-ups and they were working with redundant servers to guarantee either quick recovery or destruction of data in case they were apprehended by the police.

couldn't even imagine in your own country... Well logically you are going to do it. (GCEX, C2<sup>xvi</sup>)

NPEX2 talked about the creator the "Police Porn Virus" in similar terms:

It's a bit of a remote city there in Russia. There weren't many possibilities, I think that not even economic nor anything at all, and then this solution ... People that technically are good at computing, programming virus and whatnot, well it's a very profitable solution to their skills, because the job it can secure working as an engineer or IT consultant there in Russia, or the benefits you can obtain from an enterprise of this type, well it has nothing to do. (NPEX2, C13<sup>xvii</sup>)

However, from a Foucauldian analysis point of view (Gibbs, 2015), certain relevant issues might be underlying in terms of power structures and social control: the identification of the criminal as alien (as in different and foreign). As was discussed above, in relation to social class, this understanding of what "foreigners" are able to do in dire circumstances, can create a "developing Europe versus developed Europe discourse". In a manner of speaking, law enforcement agents might be tainting their accounts from their economic and social Spanish background. Bauman (2000) explains ideas of *antropoemic* and *anthropophagic* strategies in dealing with "others", "otherness" and "foreigners" (p. 101). By *antropoemic* Lévi-Strauss (cited in Bauman, 2000) means strategies devoted to annihilating the "other", "incurably strange and alien" (p. 101) and by *anthropophagic* he is referring to digesting their "otherness" in order to "metabolize" it (p. 101). In these narratives, a veiled *entropoemic* discourse seemed to unravel, in terms of highlighting the "otherness" of the criminal and especially the criminal foreigner, even if indicating understanding of the criminal and his/her circumstances

In both cases of designer malware (C13 and C14), “The Police Porn Virus” and “*Cryptolocker*”, the virus created an elaborate deception that implied the payment of a ransom in order to recover the computer, be it from what was a supposed “police seize” of the data or the encryption. Both were regarded as complex schemes, quite sophisticated in terms of both their design and deployment. The Police Porn Virus is presented as a “good product” (NPEX2, C13<sup>xviii</sup>) for reasons such as “the deceit was well thought through in the sense that the infection stemmed from web-pages where pornographic content was displayed” (NPEX2, C13<sup>xix</sup>) and “they [the criminal organisation] had a good virus because it wasn’t detected by any anti-virus” (NPEX2, C13<sup>xx</sup>). The technical infrastructure behind the virus deployment and management was also quite sophisticated as it is considered “bullet-proof hosting” (NPEX2, C13), meaning that:

it is super safe for them, because at this moment he/she says: OK. Well, he erases everything or remotely I connect to my server and erase everything and you open another one in other place, thus they are very safe services for criminals. (NPEX2, C13<sup>xxi</sup>)

According to NPEX2, the money-laundering procedure used in this kind of malware scheme was also extremely intricate as in some cases it implied payments by the victim using Bitcoin as well as Ukash and Paysafecrd codes that later required another money/code laundering process (NPEX2, C13 and C14). These skilled “career criminals” were able to design a tangled web of technical and legal deception that allowed them to function in a multinational environment and position themselves ahead of law enforcement agencies, legislators and computer experts.

A deep sense of respect and admiration for career criminals was evident in many of the interviews, with the offenders’ creativity and skills often being praised expressly or implicitly:

I have **a good product**; I want to reach as many people as possible across the world. Then, what can I do? What is something everyone visits, well child pornography web-pages, sorry pornography, not child pornography just pornography. Then, if I distribute this **good product** in pornography web-pages that a German, a Chinese, a Spaniard a Briton; whoever can visit, well what I have to do is give a credible message to that people. (NPEX2, C13<sup>xxii</sup>, emphasis added)

The term “Good product” is used three times in the interview when describing the “Police Porn Virus”. The use of such a term, for a designed virus, indicates an understanding of crime and “infection” from a capitalistic point of view. In the “market of crime”, the “Police Porn Virus” was deemed an admirable player. This idea underlines the notion – already mentioned – of entrepreneurship. Exquisite craftsmanship can also be found in the design of cyberfrauds:

It is **the mother of all frauds**, sincerely (murmuring: A most big son of a bitch). I have really have grown fond of him, because it has been so brutal and **so perfected**, everything **so studied**; I have never seen **such a perfect thing**, fraudster more **deserving of admiration** than this man, for me this is the investigation of my life. (NPEX1, C11<sup>xxiii</sup>, emphasis added)

In the above case, the words highlighted demonstrate respect. Even if NPEX1, despised what had been done morally (by referring to fraudsters as lacking of any scruple), he had to admire the complexity of what had been created, which is in fact a multi-layered fraudulent umbrella corporation.

Another manifestation of this idea of professionalization and entrepreneurship was that in many cases offenders did not act as “sole practitioners” but involved their families in their trade. No account was given as to how these “partnerships” were created or originated, or whether the investigated offender was the founder of the criminal enterprise or simply a mere

follower of a tradition. It is very important, in this study, to analyse or to address how an offender's morality can be "contagious" or how it can be shared amongst a number of related individuals. The idea of kinship seemed to be fundamental in the construction of cybercriminals by law enforcement agents:

In this case it was a family relationship, **a clan**, it was a family relationship because every time there is a criminal organized structure what we have detected is that there **is a strong relationship or a close and strong trusting**, generally it is **generated in families**. (NPEX1, C10 also mentioned in C11<sup>xxiv</sup>)

It was **a Russian family clan**, based here, it was the father, the son, the father's girlfriend's son and the girlfriends of both sons, I mean, totally a closed family clan, **they had this way of living** and this business model. (NPEX2, C13 also mentioned in C14<sup>xxv</sup>)

It is important to highlight how two of the interviewees used the word "clan" to define the cyber-offenders family relationship. Even though the interviews took place in Spanish, this word has the same meaning both in English and Spanish. It could be inferred that interviewees wanted to emphasize the exclusive, close-knit and outlandish relationship between members. Perhaps because social bonds forged and glued through crime could be understood as more solid, a collective experience in the family consciousness stemming from structural and social disadvantageous situations. NPEX1 used "gypsy clans"<sup>20</sup> to illustrate the kind of criminal relationships forged between families.

NPX2 pointed out that these "clans" forge alliances and collaborate with other clans. This was seen in one of the designer malware cases ("*Cyptolocker*", C14) where the indicated clan collaborated with another Russian family in order to launder proceeds of crime "evidently

---

<sup>20</sup> In Spain, some gypsy clans are specialised in drug trafficking.

because of the language and the much easier communication” (NPEX2, C14<sup>xxvi</sup>). Once again a market reference was made, this time in the interviewee’s reference to the offenders’ “business model” (see also Europol, 2015).

### 5.1.2. Fraudsters without remorse

The elaboration of the fraudster’ personality seemed to have more specific traits than the regular “professional criminal”. Fraudsters are, according to the academic literature, deemed to have a very specific set of personality traits that emphasise an over-acquisitive personality (Herrero Herro, 2007; Gavin, 2014). This is an assessment that is shared by NPEX1, who provided a very thorough description of two cyber-fraud cases (C10 and C11). These cases are of essential for this study given that they were new forms of fraud that deviate from traditional “phishing” (C3 is a phishing case, for example) or “Nigerian scam” schema. C10 refers to an online gambling fraud, which involved a bogus betting webpage, whereas C11 was an extremely complex fraud case with on-line and off-line elements that involved the creation of a fake network of police magazines in order to obtain money from fraudulent advertising.

When referring to the three brothers that set the fraudulent gambling webpage, NPEX1 claimed that:

The profile of the fraudster is a **remorseless person**, a **disproportionate motivation for economic gain**. They are usually very **intelligent and smart** people and **very creative**.  
(NPEX1, C10<sup>xxvii</sup>, emphasis added)

Then, when talking about the perpetrator of C11:

Well, the profile of a total fraudster, with a **disproportionate motivation for economic gain, fraud as a way of living**, the acting in **connivance with people from their circle of trust**, family members or close friends...A very **controlling person, very smart and intelligent**, because in order to do this and to have control over the smallest detail of anything you have to be a very intelligent person. (NPEX1, C11<sup>xxviii</sup>, emphasis added)

NPEX1 also expressed (as indicated in previous paragraphs) that the aforementioned fraudster was deserving of respect as well as “a most big son of a bitch”. According to NPEX1, the economic motivation is disproportionate, unlike other criminals that might be motivated by economic gain, and it seems to be linked to the absence of remorse that could indicate a very specific moral make-up in relation to cyberfraudsters - close to a psychopathic personality. Also, both descriptions (C10, C11) are almost identical within NPEX1’s discourse. NPEX1 might not be elaborating from a personal or professional point of view, but reciting a criminological “mantra” learnt from his studies and police education. The use of the word “connivance” (in Spanish “*connivencia*”) is legal jargon and could be an indicative of the reciting of learnt crime concepts.

Herrero Herrero (2007) describes the psychosocial profile of white-collar criminals as materialist, selfish and narcissistic, pragmatic, smart, socially adaptable, elusive to moral feelings and cynical (p. 769). Garrido, Stangeland, Redondo, and Beristain (2013) summarise different approaches to White-Collar Crime and explain the triangle of fraud; involving the existence of opportunity, necessity and rationalisation, and they also draw attention to current research that indicates that fraudsters are narcissistic individuals with low self-control. The idea of neutralisation techniques becomes extremely relevant when explaining fraud psychology (Garrido, Stangeland, Redondo, & Beristain, 2013, pp- 789-794, citing Cressey & Coleman (2001); Bromberg, 1965; Hogan & Hogan, 2001; Gottfredson & Hirschi, 1990).



Gavin (2014) analyses the psychology of White-Collar Crime highlighting the various characteristics of fraudster that have emerged in the literature:

- Clever and confident
- Ego-challenge
- The attraction of power, wealth and the desire to possess
- Might rank highly in psychopathy scales, as well as in dimensions such as charisma, communication skills and creativity
- Narcissism and the impossibility to empathise with others
- Employment or rationalisations (neutralisation techniques)

All of the above are consistent with NPEX1's discourse on the profile of the fraudster, yet this sheds no light on the persona of the cyberfraudster, as an autonomous and specific type of offender. However, Gavin (2014) explains that in e-mail frauds; "There is little social interaction and hence few social cues are given to the offender. It is this that leads to a reduction in the influence of norms and constraints" (p.212). Once again, the idea of the criminogenic architecture of the Internet is taken into account when considering its interaction with the individual.

Professional thieves - including fraudsters or confidence men - were studied by Sutherland (1937), leading to the foundations of the differential association theory. What Sutherland (1937) argued, after analysing the biographical account of a professional thief, is that "the profession of theft ... is organized around the effort to secure money with relative safety" (p. 217). Some of the characteristics of cybercriminals mentioned by interviewees (in the case

studies) are linked to Sutherland's (1937) exposition of the characteristics of professional thieves:

- Technical skill
- Belonging to an exclusive group
- Immunity from punishment (including monopoly and being used as agents of the state)
- A body of knowledge transmitted by mentoring

In terms of the above list of characteristics, "belonging to an exclusive group" and "technical skill" have both featured in the case studies - not only in relation to fraudsters but also hackers. "Immunity from punishment" also featured in the case studies in the sense that the virus designers collaborated with law enforcement agents by confessing and helping law enforcement agents investigate other criminals (C13, C14). By contrast, "a body of knowledge transmitted by mentoring" were not expressly mentioned in the interviews.

Studies by KPMG (2011) indicate that corporate fraudsters are motivated by greed ("the desire for financial gain"), work pressures (like having to achieved a certain set of targets) and the exploitation of weak internal controls (pp.9-11; see also KPMG, 2007 for previous results). The findings of KPMG's (2011) work seem to be consistent with PSEX's views on company fraud with his stating that "disloyal competence" and "disclosure" tend to be the most common frauds taking place in the private sector, because of an economic drive or motivated by curiosity (PSEX, C7 and C9). Essentially, these offences are committed by disgruntled employees exploiting weak controls or because of the lack of computer security awareness by executives and employees (PSEX, C7 and C9). In these cases (C7, C9), PSEX highlighted opportunistic and economic elements but did not make any remarks on psychological factors, such as empathy.

### 5.1.3. Hacker morality

When talking about C1, GCEX elaborated on the idea of hacker morality by offering an exculpatory discourse in terms of morality:

The hacker is **not a bad person**, let this be clear what the concept of a hacker is, not a criminal, I mean not all hackers are criminals. I mean, they are people longing for knowledge that want to know things and are very committed to the matter of information security and they like discovering different flaws. (GCEX, C1<sup>xxix</sup>, emphasis added)

There is no evidence that can support whether this is solely GCEX's perception of hacker morality or is a more wide-spread conception, even assumed by all of the law enforcement agents in Spain.

In this case, GCEX seemed to be talking about ethical hackers, those devoted professionally and ideologically to discovering security flaws and loopholes in order to share them with "the interested party or the Security Corps" (GCEX, C1). The offender's behavior, according to this construction, could be likened to the work of someone employed as a security consultant, for example. These people - ethical hackers – are seen, at least by GCEX, as extremely skilled and longing for an esoteric knowledge that might require the breach of a thin moral or legal line in order to be acquired. GCEX finished the discourse on hacker morality by adding "the concept of a hacker is **not always** a bad person, OK?" (GCEX, C1<sup>xxx</sup>, emphasis added).

GCEX seemed to contemplate the idea that there might be two types of hacker: those mentioned in the account above - helping others by using their “mystical” knowledge; and some breed of evil hacker - working for a malignant purpose. In GCEX’s account of C1, the portrayal of the hacker did not seem to be very positive one, as the narration described a chain of hackers (not a network or an organized crime, more similar to outsourcers) who created, sold and modified software in order to create a “Botnet”. *The Botnet* was described as an interlinked set of slave computers managed through a console with criminal purposes (for example, Denial of Service Attacks). This network is comprised of thousands of computers that are infected with “zombie malware” in order to control them, unbeknown to the owner or user.

That *Botnet* is considered a product that is part of the “market” and that the “end is always economic” (GCEX, C1 also referred in C3<sup>xxxi</sup>). Therefore, some hackers might consider putting their intellectual skills and drive for the obtaining of an economic gain by illicit means. It seems that hacker morality moves in shades of grey following GCEX’s accounts.

The idea of identity construction amongst hackers has been studied by Sherry Turkle (2005) and Orly Turgeman-Goldschmidt (2011). Turgeman-Goldschmidt (2011) refers to “good” (pp. 38-40) and “bad” (pp. 40-43) hackers, and the transition period from bad hacker to pro-social individual (pp. 43-4). On the other hand, Turkle (2005) talks about the hacker culture that “supports them as holders of an esoteric knowledge and defenders of the purity of computation” (p. 191). She then elaborates by indicating that it is “a culture of mastery and individualism that values complexity and risk in relationships with things, and seeks simplicity and safety in relationships with people” (p. 205).

The moral duality of the hacking culture is exemplified by the qualities and motivations of “good hackers” and “bad hackers”:

Good hackers do not feel the desire to engage in computer break-in because they are usually engaged in other activities that yield the same results, recognition, and esteem for their abilities. (Turgeman-Goldschmidt, 2011, p.39)

This is in contrast to bad hackers who “described themselves as having a wild and gifted persona” (2011, p. 40). However, “bad hackers” do not accept the deviant label (p. 41) and sometimes criticise the link established between hacking and cybercrime (Turtle, 2005, p. 214). Also, “bad hackers” do not usually have problems when combining their deviant identity into a non-deviant identity as these offenders regard their activities as “pranks” or “mischief” (Turgeman-Goldschmidt, 2011, p. 44) and the label of computer criminals is “branded by the law” (p. 44). In conclusion, “they have no moral problem with hacking itself or with their status as ex-hackers” (p. 44).

Nowadays, hacker (“good”) culture is gaining mainstream recognition through regular “*hakathon*” festivals - nothing more than programmed reunions and events, with food, drink and the promise of excitement, fun and networking (and registrations that cost exorbitant prices). *The Droidcon 2014 Hackathon* for example, was advertised as follows:

This hack will attract some of the most talented coders and creative experts – like you!  
And you’ll have the chance to work together and create something amazing. So come along to watch, learn and get stuck right into some hardcore hacking! (Skills Matter, 2014)

Going back to the interviews, NPEX2 also talked about hackers, as mentioned before (designer malware in C13 and C14), yet the economic gain seemed to be the only motivation in these scenarios. There is, however, a hacker account that calls for a more complex moral standpoint. Those are C15 and C16. Especially complex in terms of hacker morality is C15: the Spanish cell of world-wide movement “Anonymous”.

#### **5.1.4. Child sex offenders and “internet monsters”**

Many of the cases that were dealt with by interviewees related to child sex abuse or child pornography use on the internet. C2 involved a network of prostitution organised by “consenting” minors using social networks and enables offending to be explored from both the victim’s point of view and the sex offender’s point of view. C4 and C18 enabled an examination of the “*Nannysex*” case from two different sources (PSEX and NPEX3). It should be noted that the “*Nannysex*” case has become part of Spanish crime culture and it shocked the general population as it involved the abuse of babies and on online commercial basis by a Spanish paedophile ring. “*Nannysex*” was the online moniker of the head of this ring. C19 was a similar case that involved small children in a deep web based exchange community and C20 was a child sexual grooming case. The internet, according to NPEX3, has fostered the possibilities of creating links between paedophiles:

On the Internet what is, and well it is very consolidated, the creation of a paedophile community. A paedophile community that protects them, supports them, makes them see that what they are doing is not bad. (NPEX3, C18<sup>xxxii</sup>)

NPEX3’s insights on these cases was extremely relevant given that he worked as the leader of the Child Protection Unit at the Spanish National Police and had amassed an immense body of knowledge in the investigation of these crimes, as well as leading the aforementioned

investigations. It is unclear as to what was PSEX's involvement in the investigation of C4 as a former police officer and his/her accounts might stem from personal experience, general knowledge or indirect second-hand testimony. It is worth mentioning that when talking about different neutralisations used by pedophiles, NPEX3 indicated that he "was completely convinced they believed what they say". This affirmation is relevant in terms of the depth and realism of NPEX3's discourse, as some other interviewees, like NPEX1 and GCEX, were more critical towards the neutralisation used by criminals, in some cases labelling them as spurious or farcical.

PSEX and NPEX3 were asked about the reasons for the commission of crimes and the rationalisations behind the actions of people abusing children, recording abuse or sharing the aforementioned abuse on the internet. One of the most relevant and detailed explanations was given by NPEX3, when explaining the existence of a "community" that served to justify paedophile behavior on the internet. The community offers the following justifications:

That is just **another sexual act**, that the **sexuality of children has to be taught by an adult**, and well that **the love in between children and adults is possible**, all that things, that **sexuality is born since we are babies** and well that **is not a major issue to perform sexual acts with children**. (NPEX3, C18<sup>xxxiii</sup>, emphasis added)

Such faceless, internet communities were said to work as a support group, providing almost some sort of psycho-social manifesto in relation to the abuse of children. In addition, GCEX indicated that some of the child abusers investigated "tried to justify themselves like if the act they are performing is something normal and is something natural" (GCEX, C2<sup>xxxiv</sup>).

NPEX3 elaborated on other justifications used by “*Nannysex’s*” child sex abuser co-offenders by explaining that one of the offenders said “I am playing” (NPEX3, C18<sup>xxxv</sup>) when shown by the judge videos of him penetrating a child anally. Also, it was reported that many child groomers and child sex offender blame the victim. Nannysex indicated, for example that “they blame it all on me, but they let the child go naked at home” (NPEX3, C18<sup>xxxvi</sup>), yet NPEX3 added that the narrative was very common in many of the sex offenders he investigated.

The use of the concept cognitive distortions (or cognitions) can be misleading, given the breadth of the construct. Guglielmo (2015) critiques the concept, arguing that it comprises plenty of sub-categories and has become extremely open-ended. Maruna and Mann (2006) seem to have similar concern. After conducting meta-analysis, Guglielmo (2015) tries to integrate the majority of current definitions of cognitive distortions into a single working instrument:

Cognition x is distorted if and only if 1) it possesses at least one type of problematic property, which must be identified, and which is associated with clinically relevant distress, 2) it possesses a specifiable operational status, and 3) it demonstrates a domain relevant scope. (p. 74)

Hence, the idea of “clinically relevant distress” indicates that the term belongs in the realms of psychology or even criminal psychology, yet it is not an inherently criminological term, therefore difficult to apply to the SAT-RI. Maruna and Mann (2006) examined the literature to ascertain whether cognitive distortions preceded and facilitated offending, or occurred as an ex-post mechanism. They criticised the ideas of Sykes and Matza (used in this research adjacent to Wikström’s Situational Action Theory (2006; 2010, Wikström and Treiber, 2007; Wikström and Treiber, 2009) “that excuses precede and lead to offending (as opposed to just following it)” (p. 160). This has proven to be problematic as, according to the Maruna and



Mann (2006) there is not enough empirical evidence on the matter and they add that: “moreover, the cognitive distortion label is used to group together far different phenomena such as attitudes, cognitive products and post hoc excuses” (p. 161). Even so, this thesis explores the idea that there exist certain narratives inherent in cybercriminals that shield against perceptions of moral reproach. Many of these neutralisations can stem in some cases by certain social imperatives like acquisitiveness.

It may be that the concepts of cognitive distortion and neutralisation techniques are dissimilar, and in terms of the present study and the development of the theoretical model, they should be treated as different concepts yet offering the same result (the excusing from crime and the morally protective discourse facilitating engagement). This theoretical assumption can be somehow considered a weakness of this thesis, but originates from what has been mentioned before, the absence of agreement in the literature on matters relating to cognitive distortions (and neutralisations up to a point). Also, the present work does not aim to be a comprehensive study on criminal psychology (or the psychology of sex offending) but the development of a general cybercrime theory.

Boer, Merdian, Wilson, Thakker, and Curtis (2014) tried to shed light on the cognitive distortions used by child pornography offenders and contact sex offenders, through their use and revision of tools designed to measure different components of cognitive distortions (cognitions) for child sex offenders. The meta-components, and individual items of which they were composed, which they identified, included the following: “sexual objectification of children” (children as consensual partners, denial of harm, sex as an expression of love and free will) (p. 985); “justification” (blame attribution) (p. 985); “children as sexual agents” (children as sexually active) (p. 985); “denial of sex offender status” (ability to minimize the

harm or denial of control over the situation) (p. 985); “emphasis on cognitive element” (some understanding of the negativity of one’s action) (p.985); “power and entitlement” (pp. 985-986); and the so-called “component 7” (based solely on the item “My daughter [son] or other young child know that I will still love her [him] even if she [he] refuses to be sexual with me” (p. 986). Boer et al. (2014) indicated that child pornography offenders might use specific cognitions and the development of a specific scale might be needed in order to measure the specific use of cognitive distortions by these offenders (p. 988). Burn and Brown (2006) reviewed different theories of child sexual abuse and stated that “these implicit theories are identified as similar to scientific theories in that they are used by individuals to explain, predict, and interpret interpersonal situations” (p. 228). The authors advocate for the relevance of these cognitions during the whole of the offending process not as a mere ex-post mechanism (p. 228). Cognitions, therefore, are relevant before, during and after the offence.

NPEX3’s explanation of the overall schema of cognitions, reflects what has been researched and discussed in the academic literature. The idea of children being attributed sexual capacity and agency, by offenders, is mentioned several times by NPEX3, even the idea of them being blamed by the offender. NPEX also reports offender’s normalising or minimising the impact of their actions “sexuality has to be taught by an adult”, “it’s another sexual option” or it’s “no major issue”. Offenders sometimes constructed their behavior in romantic terms: “love can exist between an adult and a child”. NPEX3’s discourse seemed to offer a professional account of child sex abuse that is consistent with literature on that matter, moreover, at some points a certain patchwork of professional experience and academic literature might emerge in relation to NPEX3’s views. In addition, NPEX3 - like NPEX2, and in some instances NPEX1 - based his explanations of cases on investigative evidence (such as pictures, which he shared with the present researcher).

According to NPEX3, the existence of the internet has fostered the creation and sustenance of these cognitions underlying child sexual offending. He stated that in his extensive professional experience, child sex offenders were prone to asking for treatment or even committing suicide when apprehended before the internet became widespread. In contrast, with the arrival of the internet, child sexual abuse (in terms of the sharing of pornography) has increased dramatically and the sense of identity within this community has become bolstered. NPEX3 also warned that “organised crime has entered into the production of child pornography, which is very grave” (NPEX3, C18<sup>xxxvii</sup>). This is also in accordance with PSEX’s accounts of how the internet has facilitated access to children by people with that “appetite”, a mere “click” away, as “you don’t have to go looking for them there on the street” (PSEX, C4<sup>xxxviii</sup>).

Boer et al. (2014) differentiated between child pornography offenders, contact sex offenders or multiple offenders in relation to child sexual abuse. It must be taken into account that in C18 and C19, extensively explained by NPEX3 the offenders were involved in the creation, consumption, trading and producing of child pornography. As mentioned before NPEX3, explained the “*Nannysex*” (C19 and in lesser detail C4) case as a paedophile ring involving other sex abusers that also performed penetrative sex on children. In the “*Nannysex*” case, a new narrative emerged relating to this child sex offender’s morality and his being labelled “a monster”, not by society, or even the interviewee, but by other child sex offenders. Following NPEX3, other offenders investigated or imprisoned told the police how much they despised what “*Nannysex*” had done. “*Nannysex*” was presented as an extreme character, with a liking for sexually penetrating babies, and recording it for his pleasure and then trading these images. During the interview, NPEX3 performed a cache search in a browser and found the following message, written by someone called *Nannysex*:

Why do you want to see naked children? I do not understand .... is it to avoid the cold turkey of seeing them in action? Why watch pictures from 30 years ago? If you could be watching current pictures, you who are addicted to children, or what, do you believe that because they are lighter those pictures are not illegal? Well, yes they are. Maybe not as much, but they still are. Well, go fuck yourselves hard! (NPEX3, C18<sup>xxxix</sup>, message found in online cache)

Given the extreme nature of this case, the following conversation took place during the semi-structured interview:

Jorge: Normally for them, is it the same to abuse such a very small child? Or are there like differences or castes or strata between people that abuse smaller children, pre-adolescents, babies? Or is it seen the same way?

NPEX3: No, no, them in the paedophile world, when we had the first notice of '*Nannysex*' he was considered [by other child sex offenders] a monster. (NPEX3, C18)

The above exchange seemed to point towards the existence of a moral scale between child sex abusers, depending on the age of the children they abused. Whilst paedophiles are constructed and fabricated as monsters by the general public, "*Nannysex*" was deemed to be way too extreme by other paedophiles, as he abused babies. NPEX3 implied that "The Chameleon", the cybergroomer from C20, was also a "monster" (he referred to him as "big time tosser"), explaining that the state of his victims after the continuous and escalating abuse they experienced was "heart-wrenching".

This is very relevant information for the present study as it relates to the practice of moral qualities being ascribed by criminals to other criminals, law enforcement agents to criminals, and individual criminals to themselves. In fact, the very essence of neutralisation techniques -

discussed earlier during the exposition of the literature review to this study - is that criminals envy and participate from common bourgeoisie morality, hence the necessity of justifying what they have done according to those standards. This allows criminals to rate themselves as less morally noxious than others, or to rate other criminals as more perverse or depraved.

One of the issues raised by this account is whether NPEX3 views were purely professional or whether he was also transmitting his own personal feelings towards the offender. Even more so, was he expressing not his own feelings but acting as a vehicle for the repulse of the whole of Spanish society. As indicated above, the “*Nannysex*” case was etched into Spanish cultural consciousness, as one of the most striking and abhorrent child sexual abuse cases ever.

## **5.2. Offender Neutralisations**

As indicated during this work, neutralisation techniques are a fundamental part of the SAT-RI. All of the interviewees talked about the use of these scripts, even without being asked about them. Six neutralisation techniques were identified by the researcher (some of them differing from the list of the eight chosen for the online survey). There were a number of reasons for these differences. First, the techniques used in the online survey were identified by the present researcher, based on his review of the literature, and before the design of the survey was finalized. The researcher, in drawing up this list, aimed to make it as comprehensive as possible, giving participants as much choice as possible. By contrast, during the interviews stage, the scripts emerged “ex post” and usually in an impromptu manner as interviewees were asked broadly about what offenders told them and how they justified their actions. Interviewees tended to highlight justifications that were somewhat different to those

identified – through the literature - for the online survey. (The term “neutralisation techniques” was not used, by the researcher, during these interviews.) It became evident, moreover, in the course of the interviews that offenders developed “ad hoc” justifications tailored to the particular case in which they had been involved (for example the on-line prostitution case, C2: robust heterosexual identity) that were not considered within criminological literature. That said, a notion similar to the concept of non-neutralisation - what was coded as “it’s not justified” in the online survey - did emerge in the course of the interviews, and which has been referred “indifferent attitude”.

Once again, the idea of police culture (as explained below) has to be borne in mind, given that these are indirect accounts by law enforcement agents. Some of the interviewees (in some cases NPEX1 or GCEX) believed that offenders were simply lying when affirming statements such as “I haven’t done anything wrong”. It was not possible to determine the truth behind these statements made by offenders; in other words, it is complex unravelling whether: offenders were lying; offenders believed what they did was not wrong; or law enforcement agents believed offenders to be lying. In order to accommodate all accounts made by the interviewees, the code “indifferent attitude” was created to contain the narratives of offenders who seemed simply not to care about either their actions or being apprehended.

### 5.2.1. Denial of injury

In this type of case, offenders tried to minimise the effects that their offending had upon others or upon society. It can be argued that the differences between “denial of crime” and “denial of injury” are blurry. The idea of denial of crime seems to be oriented towards the script of “I haven’t done anything bad at all” or “what I did it’s not really a crime”, whereas in “denial of injury” accounts, a certain level of acceptance (of wrong-doing) seems to be at work, albeit with the consequences of the crime being “dulcified”.

One of the clearest examples of “denial of injury” was provided by NPEX2, when talking about the response from the “Police Porn Virus” creator (C13), when he was apprehended and questioned by the police:

**He knows it’s not right**, but well he sees it as if, what he said was: I haven’t killed anyone, I’m not a killer, I’m not a drug dealer. What I mean, **he didn’t see it as a crime, or under his conscience as a serious crime**. That is what he said; I’m not a drug dealer, ok? I’ll pay for what I have done but, fuck! I don’t understand why this is so serious or this penalty so much, because I am not.... I haven’t killed anyone; I’m not a drug dealer.... **He didn’t have the perception that it was a violent crime**. (NPEX2, C13<sup>xl</sup>, emphasis added)

In this case, the offender accepted the blame - “I’ll pay for what I have done”, “He knows it’s not right” - but he needed to protect his non-criminal identity by resorting to comparisons in scales of wrongfulness and harm. He had created a ransomware scam to earn some money, but he did not commit what he understood to be a serious crime (homicide and drug trafficking). In this way offenders are able to integrate their acts into the values of common middle-class morality, by accepting these moral scales. The problem in this account is the

reliability of what has been said as a “testimonial”, where NPEX2 acted as “proxy”. There are, though, two elements of this report that led the researcher to believe that what he said was correct. First, NPEX2 repeated the same idea in various paragraphs (part of it can be seen on the excerpt of the interview reproduced above). Secondly, NPEX2 explained that he had participated in the direct examination of the offender and forged a long-lasting “working” relationship with him – both of which should have meant that he had a good insight into the offender’s motivation. A similar narrative was encountered in the “*Nannysex*” case (C18) with references to the “monster” code, and “different” child sex offenders rating themselves (and others) along different points of the morality scale.

In other cases, the same narrative is found where, in a manner of sorts, the offender assumes the commission of a crime but, at the very same time, tries to trivialise it. In case C16 (“Latin Hackteam”) the offenders dedicated their time to “defacing” certain webpages and then sharing their deeds on-line in a hacking community. NPEX2 reported that the offenders, when apprehended, claimed “but we never did any harm” (NPEX2, C16<sup>xli</sup>). According to NPEX2, this group of hackers recognized their hacking activities (the manipulating of webpages and images) but argued that “[I] could have accessed more data, but I don’t go any further” (NPEX2, C16<sup>xlii</sup>). Apparently, they had the skills to wreak online havoc by stealing information, but they decided simply to “deface” different webpages and brag in a private online community about their actions. This seems to be congruent with the ideas presented earlier about hacker morality, and hackers’ curious and playful attitude, as if they were hobgoblins of the internet with their trivial shenanigans. In C17, a minor, living in a remote Spanish village, ransomed a big corporation after stealing information from them. NPEX2 revealed that the minor was questioned by him and “he knew he was doing something illegal, but he saw it as If saying, I didn’t have the idea of doing any more harm, I wanted my money” (NPEX2, C17<sup>xliii</sup>).



One of the key elements in this conversation was the reference to “any more harm” - the minor was perfectly conscious of the consequences of stealing information from a big company (according to NPEX2, he has performed the same scheme before and successfully so), but the economic drive simply overdrove his moral compass (his need for money justified any collateral damage). When questioned about the reasons for ransoming the precise figure of 2,500 € he answered simply: “I wanted to buy a bicycle” (NPEX2, C17<sup>xliv</sup>). In his previous cybercrime, the minor obtained a state of the art smart phone from another company he ransomed. A narrative in terms of minors and consumerism emerges if C2 is also considered (children selling sex in exchange of small amounts of money or commodities).

The ones between 12, 10; between 10 and 13, those were not aware of what they were doing, simply well... They are going to get 50 €, a Playstation and that is all, it is of no consequence. (GCEX, C2<sup>xlv</sup>)

Money and goods, therefore became an easy way to justify the harm that can result from crime, whether for the individual offender’s own well-being or for society.

By contrast, PSEX criticised the “culture of free”, explaining how individuals were not aware of the industry behind, for example, copyright and cultural creation. He argued, through his discourse, that individuals find it much easier to download movies or books (for free) than going to the cinema, because it is extremely expensive and “we are in a [financial] crisis” (PSEX, no case<sup>xlvi</sup>). It was difficult to ascertain whether PSEX was applying this justification to himself, onto others or being extremely critical about the damage caused to the entertainment industry by piracy. All in all, any of the aforementioned approaches are consistent with the literature and data collected on internet illegal downloads. This calls for a deeper examination in terms of a critical analysis, which will be carried out in the final chapter, when considering the online survey and interview data as a whole.

### 5.2.2. Denial of crime

This technique is extensively developed in NPEX1's account of cyber-fraudsters (C10 and C11), in many cases can complement "denial of injury". As indicated above, NPEX1 described the fraudster identity as being devious and lacking in empathy. The techniques presented in this epigraph support this view. In relation to C10 (online gambling scheme), NPEX1 said the following of the offenders:

Well, when you detain them all, they do not know what you are talking about, they do not know what you are investigating, **evidently they haven't done anything**, they only have a legal business that went wrong and they show no remorse, and they **do not even recognize the harm they have done**. (NPEX1, C10<sup>xlvii</sup>, emphasis added)

This "I haven't done anything" narrative seemed to appear in all of the other interviews (GCEX, PSEX, NPEX2, and NPEX3) at some point. However, it was more related with what has been called "Indifferent Attitude", which relates to an obtrusive, detached, cold and farcical attitude towards police work, embedded in the idea of "criminal career" and part of the "game" (the eternal criminal/police struggle). In order for this narrative to work as a proper neutralisation technique, it needed to be believed to some extent by the offender, as it worked as a moral shield. In these cases, one could argue that this is just usual criminal behavior, that is a tactic in a legal sense; preparation for any future legal action against the offender (no admission of facts). Even so, it is important to consider that offenders might not have been entirely sure or aware of the consequences of their acts, and even though there is a present mantra that needed to be recited in front of police officers, it can become fixated in their minds.

**Evidently**, he said that this was not a crime, that it was a legal business, that he was a company man that employed too many people, that he did a great social job because thanks to him there were too many people working. (NPEX1, C11<sup>xlviii</sup>, emphasis added)

The paragraph above refers to the creation of the attitude of the fraudster depicted in C11; the creator of an extremely intricate schema that involved on-line police magazines and advertising. The set-up involved companies within companies and an interlinked structure that supposed a real challenge for police officers to investigate. When the fraudster was apprehended (and it should be noted, once again, that NPEX1 praised his intelligence and skills) he stated that all his activities were parts of a legal business. He added that his business helped many people in dire economic situations. When questioned about whether or not the employees in the pseudo-criminal companies knew what they were doing was illegal NPEX1 indicated that “they knew somehow” (NPEX1, C11<sup>xlix</sup>) but they kept on working there.

The following is a statement in NPEX1’s interview, after being questioned about the nature of the statements printed above:

Jorge: But as a lie for an audience or for himself?

NPEX1: No. A lie for an audience, what happens is that the moment this is illegal and criminal everything falls apart, I mean he would be recognizing the existence of a crime. (C11<sup>l</sup>)

Lying is compulsory for the majority of cybercriminals (following NPEX1); otherwise it would indicate the admission of a crime and have legal repercussions. This becomes a matter of strategy in order to prepare the possible trial.

In addition, PSEX pointed out the following when he spoke about people stealing Wi-Fi signal:

People do it, but well, really, the commission of said crime is there. Nowadays there is nothing stipulated but we would be stealing or hacking the cost of the Wi-Fi, that amounts for a monthly 30/40 € let's say, that type of crime, well people **say: Noooooo this is nothing and I do it** and sometimes because of the simple fact that I am good at hacking the neighbour's Wi-Fi. (PSEX, no case<sup>li</sup>, emphasis added)

This is very similar to what was elaborated before on illegal downloading, and can easily be related to the general sense of normlessness that populates the internet. Individuals might believe that stealing Wi-Fi is not a crime, especially because of how easy it has become for the general public; they can do it even by downloading mobile applications (according to PSEX).

On the other hand, from a critical standpoint there might be a subtextual power abuse, the police acting as agents of control, understanding criminals oversimplistically as scheming liars. Law enforcement agents like NPEX1 and GCEX affirm that offenders know what they do is not right, yet they lie about it. It would seem that law enforcement agents are taking from offenders the capacity of taking the blame, of desistance or repentance; therefore constructing a viler and deterministic view of a criminal career. At the same time, law enforcement agents spoke from their professional experience; one in which they understood the whole system of constitutional rights assisting detainees and indicted individuals.

### 5.2.3. Appeal to higher loyalties

This neutralisation technique refers to the justification of a criminal act by resorting a greater authority, or even the greater good. Offenders might indicate that they did what they had to do in order to save their country or that they were just doing justice. This technique is featured in C15 (Anonymous Spain) and serves to explain the reasons why many individuals might have joined the hacktivist crusade. Anonymous has published an online manifesto, in which it clearly states its cosmovision (world-view). People joining this “movement” presumably adhere to the core principles of this manifesto. According to the manifesto, the philosophy of Anonymous revolves around the following ideas: unrestrained access to information; rule of the people (self-governance); importance of personal privacy; the use of privacy and secrecy by institutions according to the rule of the people; and citizen responsibility in maintaining a transparent society. They then add their manta: “We are Anonymous. We are Legion. We do not Forget. We do not Forgive. Expect Us” (NPEX2, C15). They also assert that “Anonymous exist only as an idea”. One could argue that what Anonymous seek is social justice by disseminating a fairer idea of democracy and, in order to achieve it, they have resorted to using hacking.

In C15, Anonymous Spain was investigated by the police because it: published confidential information on police staff; disseminated personal information on a local politician who it believed was corrupt; and defaced institutional webpages – including a political party’s webpages, by painting fangs on politicians’ pictures. When asked why Anonymous did this, NPEX2 replied:

Firstly, I believe, that one, it is because of a motivation, **because of an ideology**. The first of them is because **he/she believes that he/she can change, that hacktivist discourse of “Anonymous” that we can change the world**, down with the corrupt, freedom when sharing information, I mean that hacktivist discourse from Anonymous. You are totally integrated, and you say, I want to collaborate with the cause; we are many the ones who want to change the world, and whatnot. (NPEX2, C15<sup>lii</sup>, emphasis added)

The above explanation is concordant with the Anonymous manifesto and it could be seen to demonstrate a belief in a higher order: a freer and more democratic world, worth fighting for; a world worth committing crimes for. However, and according to NPEX2, the motives behind all the people who were investigated were not as sublime as has been suggested above. Some of the authors involved, according to NPEX2, only wanted to take revenge on a politician they held a grudge against.

One could argue that NPEX2 was being frivolous and debasing a movement that has inspired many people to fight for constitutional rights; that he was acting as an agent of the “status quo”. However, another perspective could be that NPEX2 - and bearing in mind he had a computing engineering background – was better able to understand the movement, and his essential criticism is that individuals were using the movement as an excuse for committing crimes.

#### 5.2.4. Fun/just a game

It seemed that for some of the people who featured in these cases, the commission of a crime was just a game or was perpetrated for fun or thrills. Continuing with the Anonymous case (C15), NPEX2 explained that he believed that younger offenders joined the movement in the search for fun and for the purposes of socializing. The Anonymous platform allowed them to chat or even organize offline meetings all over Spain. It should be remembered that these assessments – of the motivations of Anonymous members – were based largely on NPEX2's beliefs and personal opinions, as was clear in his regular use of terms such as "I think" or "I imagine".

Also, according to NPEX3, "*Nannysex's*" co-offenders referred to the idea of game on several occasions. The one referred to as "D'Arcy" liked to spank children (exploiting his role as a school teacher), whereas the one named "Etex" used his situation, as a doctor, to involve his victims in sexual games. Similarly, the one known as "Todd" said "I am playing" (NPEX3, C18) when confronted with a video of himself penetrating a child.

This neutralisation technique is very complex to analyse and comment upon. On the one hand, the idea of adolescents joining the Anonymous crusade for the purposes of "passing the time" seems a plausible idea and could help understand better the hacktivist movement. On the other hand, the "just playing" technique when applied to child sex offenders collides with the concept of cognitive distortions (cognitions).

Another case with a reference to the “game” neutralisation was found (albeit in a more implicit way) in C2, which involved minors selling sexual services via social networks, and which was discussed by GCEX. GCEX explained his assessment by pointing out that younger children (10-12) did not really understand that what they were was “sexual”, but were preoccupied with thoughts of the “easy money” and the commodities (like video-games) that they gained from their role in this offending. According to GCEX, the way these children construed their involvement was as if it was a game, where they could win desirable rewards. Maturity could, then, played a fundamental role in the design of particular neutralisation techniques. As GCEX made clear, children were not old enough to understand the “value of sex”.

#### **5.2.5. Denial of victim**

In using this neutralization technique, offenders focused blame on the victims, believing that whatever happened was partially or entirely due to their behavior. Offenders also - through their use of this technique - minimised the impact of their behavior upon victims by perceiving their crimes as victimless.

When talking about sex offenders’ cognitive distortions, the idea of blame and children agency has been already mentioned. NPEX3 indicated that “*Nannysex*” argued that it was the parents who “let the child go naked at home” (NPEX3, C18 but also referring to C19 and C20). This becomes also very relevant when describing C20, a child sexual grooming case. In this case, “The Chameleon” (he used quite a large number of online identities) pretended to be a girl in some cases, in order to gain the trust of other girls and subject them to a spiral of sexual abuse and extortion. He convinced them to send him pictures of their breasts. Once he had the pictures and had gained control over their e-mail system, computers or webcams, he



threatened the girls with deleting their Hotmail accounts, distributing their pictures or deleting their friends list. Girls were to send a specific quota of pictures, with the explicitness of these images having to increase over time. According to NPEX3, this narrative was fairly common among online child sex offenders: “No, no, it’s them [the girls] the ones provoking” (NPEX3, C20<sup>liii</sup>). It is worth pointing out that NPEX3 considered child sexual groomers also sex abusers, because of the subjugation and control over the victim.

Jorge: So groomers have even said that it was the lads or lassies’ fault

NPEX3: Yes, yes. Many times. (NPEX3, C20<sup>liv</sup>)

In the description of the aforementioned C13, NPEX2 believed that one of the reasons behind the malware designer’s use of neutralisation techniques is the he did not “see the victim” (NPEX2, C13<sup>lv</sup>), he did not have any awareness of doing something wrong and that, in a way, seem to coalesce with the denial of injury narrative already mentioned. NPEX1, also indicated implied in relation to C10 (fraudulent gambling scheme) that offenders were extremely abusive towards their victims, what also seems to connect with the interviewee’s discourse of the absence of empathy and remorse from fraudsters.

#### **5.2.6. Robust heterosexual identity**

This neutralisation technique, utilized in C2, was according to GCEX, an “ad hoc” script. GCEX explained that male children were selling themselves sexually to men, via social networks, in order to obtain money or goods. However, the children in question took an active role in limiting the extent of the sexual relationship. They did not want to be sexually penetrated or to have any other sexual act performed on them. By doing so, these children (according to GCEX) were able to justify that they were, in essence, heterosexual males.

Jorge: And why do you think the older ones did demand being the ones penetrating, yet not being penetrated? I mean, why this contradiction?

GCEX: Because as these aggressions have a homosexual nature, the concept the minor has in mind is, I'm not homosexual. The moment when I am not penetrated or I don't perform anything, I mean, I do this for money, he is aware of penetrating an adult man, ok? But his way of thinking is saying... I am not homosexual, you know? (GCEX, C2<sup>lvi</sup>)

GCEX believed that the above minors involved did not ascribe any value or importance to the sexual relationships in which they were engaged. For them, they were means to an end; the acquisition of money and desirable goods. In order to realise these goals, the minors sold sex to male adults. These homosexual practices seemed to endanger their masculinities and heterosexual identities so they created the "robust heterosexual identity" justification. This justification is relevant in social and cultural terms, as it seemed to imply a commodification of sexuality by young people and a capitalistic rationale. In this chapter, the idea of crime and deviance, as means for the acquisition of money, has been prominent. Money was the ultimate social goal; therefore morality, identity and sexuality, had to bend and be re-imagined in line with capitalism. Also, what becomes really important is the public reinforcement of their masculine identity and the necessity to justify homosexual sex in the light of a "greater good" (money). This justification is also relevant from a gender perspective, given that the idea of justifying homosexuality would imply that homosexuality itself is contemplated as deviant by the children involved.

### 5.2.7. Indifferent attitude

The last neutralisation technique that will be dealt with in this chapter is what has been coded as “indifferent attitude”. This is not a proper neutralisation technique, but rather marked the lack of such a technique. This technique is the equivalent of the “non-neutralisation” (this is not justifiable used in the online survey) and emerged during the interviews. Many of the interviewees referred to the indifferent attitudes of offenders, describing them as “non-cooperative” or “lying”, or stating that they had an accepting attitude towards being apprehended by law enforcement.

In many situations, this was a mere legal manoeuvre, with the offender attempting to protect himself from legal proceedings. In other instances, offenders “did nothing”, opting instead to remain silent or otherwise not collaborating with law enforcement. This seems to relate, in a way, to the later cultural construction of law enforcement work as a game of chess, a tournament of the minds, between criminals and law enforcement agents. Again, it must be remembered that these findings draw upon the perceptions of law enforcement agents – perceptions that might be influenced by cultural biases of these agents. Interviewees do not narrate (or are unaware of) the existence of the term and concept of neutralisation techniques in offenders.

Jorge: And The Chameleon, did you learn of his justifications, why he did it, why not? Did he say something in that regard? Maybe in between lines?

NPEX3: No, his motivations, really...They don't explicit them, except they feel guilty, they don't, in the first place he doesn't feel guilty. (NPEX3, C20<sup>lvii</sup>)

NPEX3 described a case (C19) which involved a child sex offender producing child pornography and sharing it on the internet, via the deep web. The offender indicated that that “It wasn’t him. He hasn’t done anything. But we found all the material in his house, even the dildos he made a six year old girl use” (NPEX3, C19<sup>lviii</sup>). This is also concurrent with the “I am playing” line, used by “Todd” (one of “*Nannysex’s*” co-offenders, C18) during a court hearing. At first sight these narratives might be understood as a “Denial of Crime” neutralisation, but from the context of the interview, NPEX3 wanted to signify that these individuals were non-cooperative. NPEX3 emphasised an external manifestation (of offender’ behavior) as opposed to any intersubjective assessment (of their motivation). In these situations, law enforcement agents could not glean how offenders felt inside or whether they really believed what they had said. Continuing with this theme, NPEX3 added that *Nannysex’s* co-offenders started blaming one another and that one of them “completely shuts himself down” (NPEX3, own translation<sup>lix</sup>). Moreover, “*Nannysex*” himself “doesn’t recognize it is a crime, yet he doesn’t justify either” (NPEX3, C18<sup>lx</sup>), therefore “*Nannysex’s*” attitude is understood as somehow ambivalent in regards to the investigation of the case named after him. NPEX3 went on to say that he had to empathize with “*Nannysex*” in order to trying to understand the motivations behind his acts because he also “shut himself down”. “*Nannysex*” did not want to collaborate with law enforcement agents and the investigation was put and risk.

NPEX1 believed that all cyberfraudsters were openly lying when negating the facts. However, he felt that such lies were not a mechanism for the self-protection of an offender’s moral compass but rather “a lie for an audience” (C11, see the “denial of crime” section). The C11, the designer of the online scheme “didn’t show resistance, neither collaboration” (NPEX1, C11<sup>lxi</sup>) when confronted with proceeds of his crimes by the investigators. This points, again, towards offenders lying when negating facts and being non-cooperative.

GCEX expressed something similar to what NPEX1 and NPEX3 described about offenders demonstrating an “indifferent attitude”, using the cybercriminals’ point of view:

OK, I know what I have done. If they have come so far is because they need to have more than enough evidence to get them here, but now it is the Guardia Civil the one who has to find all evidences to proof what I have committed. (C1<sup>lxii</sup>)

GCEX continued explaining offender’s indifference: “they won’t tell you the origin of the economic benefits they had, they won’t reveal who their clients are, they won’t reveal their providers” (C1<sup>lxiii</sup>). Indicating how professionalized cybercriminals have become and how they seem to be encouraged by what NPEX2 called a “perception of security” (C14<sup>lxiv</sup>).

## **5.1. (Cyber)Police Culture**

Zizek talks about ideology following a Marxist assumption:

The very concept of ideology implies a kind of basic, constitutive naiveté: the misrecognition of its own presuppositions, of its own effective conditions, a distance, a divergence between so-called social reality and our distorted representation, our false consciousness of it. (Zizek, 2008, p. 24)

This classic concept of ideology, according to Zizek (2008), works as a filter, a lens through which we experience society leading to a “misrecognition of the social reality which is part of this reality itself” (p. 25), a social fantasy where individuals find themselves immersed in unknowingly. Zizek subsequently expands on the concept of law and authority based on “external” obedience for the sake of abiding by authority as an external entity that is in itself

and by itself (not because what is to be done, or how the law is understood as good or necessary, but because it is authoritative and therefore good or necessary). Ideology and obedience can be seen as a pivotal point in understanding how police officers work under the rule of law. Section 5.1 of the Security Corps Act, which regulates the functioning of the Security Corps in Spain (including National Police and Guardia Civil), states:

Abiding by the legal order, specially:

- a) Exercise its function with absolute respect for the Constitution and the rest of the legal order (1986)

The law becomes the superior structures that ideologically and normatively rules police actions and, therefore, directs and articulates their discourse.

Following the ideological approach, Reiner (2010) contends, when talking about police culture, that “police forces in modern liberal democracies do face similar basic pressures that shape a distinctive and characteristic culture” (p.116). Reiner believes there are seven key elements that recur in police culture. These elements shape the beliefs and narratives of police officers, creating a sort of common moral ground for the majority of them. These elements are:

1. Mission-action-cynicism-pessimism
2. Suspicion
3. Isolation/Solidarity
4. Conservatism
5. Machismo
6. Racial Prejudice
7. Pragmatism

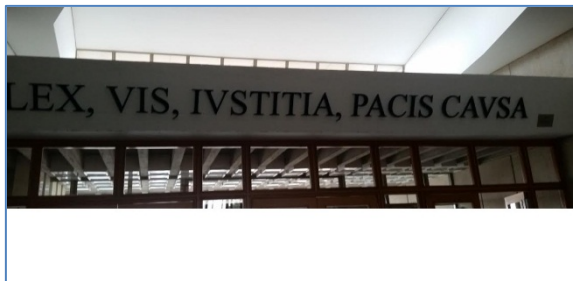
(Reiner, 2010, pp. 118-132; also Rowe, 2008, p. 102 citing Reiner, 2000)

From a critical point of view, it is important to understand how these values may have shaped police accounts of cybercriminals in Spain; first, because there might be differences in how “cyberpolice” construct criminal identities (or how highly specialized police units do), and secondly because no studies on police culture (of any sorts) have been carried out in Spain. This insight is essential in trying to understand how individuals “ascribed” to law enforcement morality, review and rate their own morality and the morality of others.

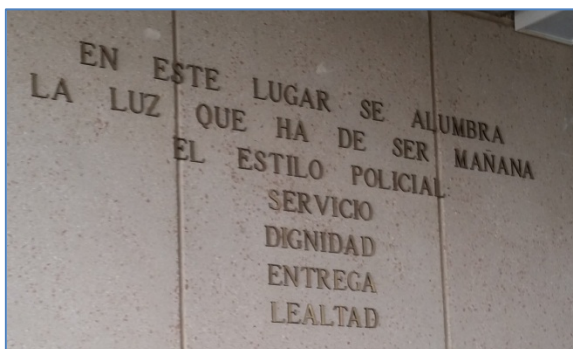
### **5.1.1. Mission- action-cynicism-pessimism**

Reiner (2010) talk about this sense of mission and how police work is “victim-centered” (p.119). At the National Police Academy in Ávila (four of the interviewees were trained at said facilities) the words engraved at the very entrance of this facility are shown in Figure 22.

**Figure 20. Spanish National Police Academy entrance**



**Figure 21. Another detail of Spanish National Police Academy entrance**



“Lex, Vis, Iustitia, Pacis Cause” (Figure 20) means “Law, Strength, Justice at the Service of Peace” whereas the wall engraving can be translated as “At this place blazes the light that is to be the policing style of tomorrow. Service. Dignity. Commitment. Loyalty” (Figure 21). The sense of mission and destiny seems to be present at a very early stage of the law enforcement career.

Following this discourse, offenders may be viewed as oppressors, and in some of the interviews, law enforcement agents refer to cybercriminals as “a most big son of a bitch<sup>lxv</sup>” (NPEX1, C11) or “*un cabrón con pintas*” (slang Spanish that could be understood as a “big time tosser”, NPEX3, C20). In relation to this sense of mission, police officers harden themselves by resorting to pessimistic and cynical attitudes. Insults (*grandísimo hijo de puta*, *cabrón con pintas*) are also used in their superlative form (*grandísimo*=big time) and even though it is very difficult to find an exact translation into English of “*cabrón*”, the word transmits the idea of a bad or ruthless person. One could argue that, by using insults, police officers position themselves in moral superiority (‘they are bad, we are good, we fight evil’) exerting a position of power as means of agents of social control - labelling undesirable deviant agents. On the other hand, the use of swear words is very common in Spain, even in formal contexts, and in some cases could ironically mean affection or familiarity, but usually they are a means of expressing masculinity. This could be something to say your male friends after meeting them randomly on the street. NPEX3 also resorted to insults, even if following a neutral and detached discourse throughout his accounts, whereas NPEX1 used a more ironical, brisk and conversational discourse. It is also possible that NPEX1 is not acting entirely cynical and by his tone, almost inaudible when insulting, it was supposed to be a “wink” to the researcher in order to create a connection.



The need for action does not seem to apply to “cybercops” as their job is desk-based, with their acting as investigators and knowledge-brokers. However, their particular views do not seem to be tainted by cynicism or pessimism, but are informed by a sense of understanding, a “social and criminal awareness”. NPEX1 indicates that you “always put yourself in other people’s place” (C10)<sup>lxvii</sup> in order to investigate criminal offences. Moreover, many of the accounts have demonstrated a high degree of empathy and understanding in terms of cyber-criminals. NPEX2 indicated how “they became friends” with one of the designer malware creators. NPEX1 felt “admiration” towards cyberfraudsters and GCEX understood how cybercrime can be a career option for some disadvantaged yet intelligent youngsters “Well, logically you are going to do it” (GCEX, C3). Also, PSEX reflected on the idea of computer illiteracy and societal change, meaning that some people are not even aware of their commission of a crime on the internet because of the absence of a “computer safety culture”. He also added a very critical approach to the fast changes that the family institution is facing because of the use of digital technologies, for example, the parent-children divide and the liquid nature of romantic relationships. It could be argued that PSEX’s narrative moved between a cynical,-pessimistic approach and a critically realist approach.

### **5.1.2. Suspicion**

This element refers to the ever-present sensation of constant suspicion that permeates police work and also to their penchant for offender stereotyping (Reiner, 2010). Interestingly enough, the interviewees were keen on breaking the stereotypes of some offenders, especially in terms of hacking and child sex abusers. GCEX commented in C1 that hackers “are not evil” or “do not fit the shy guy stereotype”. At the very same time, the interviewee GCEX tried to demystify the obscure figure of the child offender in contrast with popular depictions. On the other hand NPEX3 described only child abuse and grooming offences with professional detachment

(although in C20; a child grooming case, he/she indicated how taken aback he/she was by the emotional state of victim's or how the offender was a "big time tosser"). In addition, NPEX3 and GCEX offered very interesting insight on paedophile psychology. According to NPEX3, *Nannysex* (C18, also mentioned by PSEX as C4) was a "monster" amongst the child abuser "community" because of his abuse of babies and other extremely young children. Interestingly enough this "monster" label is not applied by the interviewees, but is accounted by them as applied by society or other sex offenders.

### **5.1.3. Isolation/solidarity**

In respect of this element, police work is presented as a "Them vs Us" (Reiner, 2010, pp. 122-16) - a sort of ever-present battle between a cohesive group (police force) against external indomitable forces. Said antagonists can be divided as follows (with only those appearing directly or indirectly in interviewee accounts are listed, with: "challengers", "disarmers", "do-gooders" and "politicians" being omitted):

- "Good-class villains" - Worthwhile of pursuit and rewarding to chase and investigate by police officers. This becomes very patent in the narratives of NPEX1 who demonstrates a professional admiration for the fraudster under investigation. Other interviewees ascribe high levels of intelligence and skills to the cyber-criminals they pursue (GCEX, NPEX2).
- "Police Property" - This refers to the idea of police being left in charge of solving a particular problem or dealing with a social group. These groups are usually social "pariahs" and the police are left to "control and segregate" (Reiner, 2010, p. 123) them. This is relevant given that the general public is not really aware of the majority

of cybercrimes being developed and committed (PSEX account is centered on that idea).

- “Rubbish” - are people who are deemed as messy or unworthy when making calls to the police (2010, p. 124), they waste police time with trivialities that do not belong to the path of higher destiny that police officers walk. The only oblique mention during the interviews was made by NPEX2 when explaining C13 (Police Porn Virus) indicating that:

We can tell anecdotes of people calling, for example on the phone, and they told us that... Fuck, I'd pay the fine without any problem. Well, well, yes, but **I think it is not a crime to watch pornography**. (NPEX2, C13<sup>lxvii</sup>, emphasis added)

And other people calling the police and indicating that:

No, no I haven't watched child pornography at any moment, I have watched this and whatnot from that webpage **but it was adult pornography** and all, I don't know why this about child pornography appears, but if the least I have to do is paying 100 €, I pay 100 €. (NPEX2, C13<sup>lxviii</sup>, emphasis added)

However, these comments do not seem to imply criticisms of victims for “bothering” the police with their petty concerns or for becoming easy prey. The researcher understood them as a humorous relief, with NPEX2 trying to explain how cleverly designed the virus was, infecting users from porn websites. Also, the tone and the use of the word “anecdote” tried to convey a sense of “vaudeville” when depicting internet users explaining to unknown police officers their pornography watching habits. This seems to add more to the empathic texture of NPEX2's account. It could be argued that NPEX2 was one of the officers that demonstrated the least judgmental

attitude and the least incisive tone, maybe because the crimes he discussed were more technical in nature and were less toxic in terms of the consequences in terms of victimization.

#### **5.1.4. Conservatism**

This element of police culture refers to the idea of police officers being conservative politically and morally (Reiner, 2010, pp. 126-128). It is an element of paramount importance in understanding police views on offenders' morality. In this study, the idea of morality and perceptions of morality takes center stage; therefore the issue of police painting their accounts with their political, religious or moral cosmovision or world-view has to be addressed thoroughly and critically.

Once the interviews were studied, in terms of wording, we can find small hints of the existence of such conservatism. However, it does not seem to be part of the integral architecture of the discourse but more a superficial coating. This moral conservatism manifested itself in a threefold manner during the interviews: by describing offenders as "evil", by describing offenders as "not so evil", and by describing current moral state of affairs as dire ("dark times"):

- **Evil** - This idea seem to be present, but not in a biblical antagonistic manner. As has been indicated above, NPEX1 refers to one fraudster as a "son of a bitch". NPEX1 also indicates that fraudsters are "remorseless" and overwhelmingly profit-driven, whereas NPEX3 calls a cybergroomer a "big time tosser". The idea of the "monster" is constructed by NPEX3 when indicating that one child sex abuser was a "monster" in the eyes of other sex abusers and how dealing with victims of cyber-grooming was

heart-wrenching. It is extremely important to mention that when NPEX3 refers to “the monster” he is (in theory) conveying the views of the child sex abuser community (or maybe society in general). It could be indicated that NPEX3’s account is detached and professional and NPEX1 is more emotionally charged with more references to cybercriminals being remorseless and evil.

- **Not so evil** - Hackers and malware designers are presented by GCEX and NPEX2 as not evil “per se”. They are seen as people with a lust for knowledge and challenge. Also, the idea of individuals who were driven to crime because of structural causes (such as poverty) seems to be present in both discourses. One could argue that this view is conservative and condescending in its simplicity: Russians are poor and they decide to commit crimes against Spaniards. NPEX2 indicates that he befriended some of the cybercriminals and he resorted to a more humorous or ironical approach during interviews with them. GCEX seemed to be more conservative when trying to describe the social class of one of the cyber-offenders in C2:

the parents came from medium-low social stratum. Well, we are not going to say they were... I mean, they lived in a humble house and in a humble neighbourhood, but it wasn’t a slum, they weren’t ... OK... They were, I mean from medium-low stratum, but not low at all. (GCEX, C2<sup>lxix</sup>)

GCEX tries very hard to justify the social class of one minor that prostituted himself by using social networks, but this description seems to be awkward and uncomfortable for the interviewee as if talking about social class was in bad taste. He does not seem to be very sure as to how to convey the idea of lower social class. This can be also understood as an exertion of power from the Guardia Civil interviewee, as he understood the world from a middle class morality and understood of crime as being linked to lower classes and strata - something more or less admitted, yet not to be

publically spoken about. The idea of social class seems, from the point of view of this account, to be something alien and pertaining to arcane police knowledge.

NPEX2 also talked about Anonymous in C15 and their defacements of political parties web-pages. Interestingly enough, the interviewee's description of the attacks and the "Anonymous" hacktivist initiative is detached and professional; no pejorative language is used when talking about them. NPEX2 is critical of offenders, when indicating that the core reason for their joining Anonymous could be ideological, but he identifies other drivers, such as revenge or "having fun" especially for youngsters who, he thinks, might view their activities as some sort of social pastime. Also, NPEX2 invites reflection when talking about Anonymous attacks one major newspaper published a new entitled "DDoS attack: Crime or protest?" (Maeztu, 2011). This article advocated that citizens fight for their rights by using cybercrime techniques and criticized the criminalization of such behaviour. Later on, as indicated by NPEX2, the major newspaper in question suffered a cyberattack and published the following headline "Far-Rightist arrested because of attacks on various digitals media" (Público, 2013) and hacktivism was presented in a less favorable manner.

- **Dark Times:** Many interviewees argued, or at least suggested, that the internet was posing a major social challenge, as it is changing many behavioural or relational paradigms.

Following that discourse on current morality, PSEX was extremely critical of current society and its relationship with the internet. His discourse elaborated ideas about how smart phones fostered infidelity or at least normalised extra-marital flirting. He

also discussed how the legal apparatus seemed to crush the powerless and benefit the powerful. This idea was linked to how companies are extremely harsh on ordinary workers (in terms of, for example, compliance, company rules and sanctions.) and too lenient on executives “many hindrances, to the people at the bottom many key-locks are put” (PSEX, no case<sup>lxx</sup>). Metaphorically and by resorting to hyperbaton, PSEX tried to emphasise what might be understood as an unfair power shift.

PSEX also criticised the idea of individuals not paying for goods and services related to the entertainment industry:

It’s not the same but well, **the culture of free** and of what I have obtained and it hasn’t cost me anything, and well, **we are in a crisis** ... he/she doesn’t have any knowledge of the whole industry behind copyright, of creator rights. (SPEX, no case<sup>lxxi</sup>, emphasis added)

References were also made to the absence of computer and security knowledge. According to PSEX, there was a generational divide that impeded parents from understanding what their children were doing on the internet. At the same time, according to this interviewee, the very same children did not understand the entirety of the dangers that loomed on the internet.

Another interesting reflection on capitalistic values and moral crisis was made by GCEX when talking about C2, and why children sold sexual services on the internet. According to this account, children trivialised sexuality and commodified it. They did not understand the inter-personal and emotional charge of sexual exchanges, and

used sex to obtain trivial goods, such as “A Playstation 3, a state of the art mobile phone that is worth 200 €, 300 €, 400 €” (GCEX, C2<sup>lxxii</sup>).

All in all, it is difficult to separate out the elements that relate to police cultural conservatism from those relating to personal moral values. Although, the majority of participants were extremely critical of society in terms of “moral drift”, they did not seem to apply this conceptualisation to cybercriminals but to internet users in general. Following this line of thought, it could be argued that the internet is a reflection of the offline society -what Baudrillard (1988) called a “simulacrum”, a copy without the original, which becomes another entity in itself. The internet could be understood as the perfect example of a simulacrum drawing from tangible reality and then creating its own structures. As such, it replicates its moral compass, accentuating some elements by its very peculiar architecture. What happens in society is to happen on the internet, yet in different ways. What can be safely indicated is that all interviewees were critical of different aspects of society and crime.

#### **5.1.5. Machismo**

No implicit accounts of machismo were dealt with during the interviews. PSEX critiques on technology changing the concept of family and relationship were presented from a masculinity of femininity perspective. Also, many of the male interviewees talked about homosexual practices without ascribing any negative aspects to them. GCEX elaborated how male child prostitutes justified their sexual identities by resorting to non-passive sexual practices.



Also, only one of the interviewees was female, yet no gender discourse seemed to permeate her account. On the other hand, it could be argued that, in some ways, she acted and presented herself as “tough girl” (not expressly). However it is not possible to discern if she ascribed to constructed male gender models, or views on female police officers as there is no data about it in Spain.

#### **5.1.6. Racial prejudice**

In relation to racial prejudice, no specific account has been made explicitly. NPEX1 mentioned that the family structure of fraud business was similar to “gypsy clans”, in a factual way. As indicated beforehand, many of the cybercriminals were based in other countries and had managed to form multi-national networks. Comments on people committing crimes because of their country of origin’s structural situation (for example, Russia) might be understood as prejudiced by some, yet the interviewees seemed to be talking about them in a purely explicative manner without ascribing negative connotations.

GCEX indicated, when talking about C1, that hackers were stereotyped as shy and reclusive people but he added that while this description could apply to Anglo-Aaxon countries it was different in Spain: “we have better weather, we have the sun and we have other circumstances that help us socialize with people” (GCEX, C1<sup>lxxiii</sup>). This comment does not seem to add anything to the discourse and could be understood as clichéd and irrelevant, maybe even chauvinistic, however, there is not enough data to support that GCEX is prejudiced towards other countries.

In addition, NPEX2 talked about forging “friendships” (better understood as “strategic alliances”) with Russian cybercriminals. Also, C16 and C17 were explained as cybercrimes perpetrated by South American individuals. C16 was organised by a group called “Latin hackteam” and C17 by a Bolivian minor living in a remote village in Asturias (Spain). When referring to the investigation of the hacking offence (information ransom) committed by this minor (C17) NPEX2 stated that:

It was a message written in **South American words**, even the e-mail account was a domain from @bolivia.com, and **because of the accent**, the attack was perpetrated by a South American. (NPEX2, C17<sup>lxxiv</sup>, emphasis added)

It is unclear as to what was meant by “South American accent” in a written e-mail, but following NPEX2’s explanation, it seems to refer to the linguistic differences between South American Spanish and Castilian Spanish. Both versions of the language are clearly distinguishable in both written and spoken format, as wording and phrasing differ. Although it is quite generic and vague to refer to “South American words”, as it does not reflect the rich particulars of many of the variations of the Spanish language, it does not seem to be overly charged with racial prejudice. It could be argued that it is quite a generic affirmation, colloquial and somehow lacking in cultural awareness.

#### **5.1.7. Pragmatism**

According to Reiner (2010) police constables had a “very pragmatic, concrete, down-to-earth, anti-theoretical perspective” (p. 131). Contrarily, the sample of interviewees demonstrated themselves to be highly motivated individuals interested in understanding crime from a less pragmatic point of view. Their long experience in the field and their current jobs (the three National Police experts were in charge of different units: Open Networks, Logic Attacks, and

Child Exploitation and Protection). NPEX1 claimed that it is important to think as the criminal would do in order to investigate cybercrime, and also advocated for the use of intelligence techniques in investigating and explaining cybercrime. NPEX3 made affirmations about online child sex offender's identities and the process of grooming, and NPEX2 was very skilled in the technical side of computing. These three interviewees worked with Europol, and were also involved in disseminating knowledge amongst colleagues and law enforcement agencies. These three interviewees had their case presentations pre-prepared, having used them previously for educational and training purposes. As indicated above, NPEX1 used extremely elaborate graphs, inspired by intelligence analysis, to guarantee a clearer investigation.

GCEX and PSEX also had very extensive experience in terms of investigation and policing more generally. Both of interviewees were extremely cautious when asked about child sex abusers, explaining that this subject raised complex psychological issues, about which they were not very knowledgeable. However, this should not lead them to be labelled as extremely pragmatic individuals but maybe cautious or humble.

#### **5.1.8. Concluding remarks on (cyber) police culture**

Talking about police culture in Spain is a complicated task. The police tend to be opaque in terms of their relations with academics and in respect of public accountability. However, a common understanding of Spanish police culture seems to exist between social researchers, even though it has not been studied.

Police officers are currently moving towards a more “public-friendly” image, by means of, in particular, social networks. (Guardia Civil and Spanish National Police both have official Twitter and YouTube accounts. The Spanish police has an official Facebook account and an Instagram account. Different local police services also have Twitter accounts). The National Spanish Police official Twitter account - @policia - has gained media and social praise and recognition because of its down to earth, humorous and, in some cases bizarre, approach to policing and crime prevention by using jokes, memes and slang. Guardia Civil has also followed that trend quite successfully. Plenty of police officers are also using personal accounts to tweet about their daily jobs (some of them have reached internet celebrity status).

Thus, considering Reiner’s (2010) construction of policing (drawn from Anglo-American policing but utilised in this thesis), it can be argued that the sample interviewed in the present study do not abide by the previously discussed maxims. Many of the agents interviewed demonstrated some of the seven elements at some point during their accounts of their work in cyberpolicing, but these elements were not the dominant mould or script of their discourse, but rather seemed to indicate fragments of the interpersonal axiology of the experts.

Having analysed all of these elements, it could be maintained that “cybercops”, at least Spanish “cybercops”, do not seem to ascribe to a specific cultural pattern. According to what Reiner (2010) calls “variations in cop culture” (pp. 132-135) - where he summarises different police approaches found in academic literature, as well as his own nomenclature - it could be contended that Spanish “cybercops” could be close to being labelled as “the professional policeman”, who are ambitious and career-conscious, with a balanced view on all the aspects of crime fighting (Reiner, 2010, p. 133; citing Reiner, 1978, chapter 12).

A new type of police culture might be emerging in Spain, one where senior police officers have a stronger social sensibility (than their peers) stemming from a life-long learning process, which involves training in disciplines, such as law, criminology, computing and psychology. These “new” police officers are also concerned about the causes of crime, the sharing and updating of investigative knowledge, and the use of intelligence and multi-disciplinary approaches. However, it is difficult to indicate whether this culture applies solely to police officers who investigate cybercrime or the newest generations of high ranking officers that perform a “desk job” rather than a “street job”. It is, therefore, not possible to conclude whether the interviewees have provided biased information, and whether this is due to the existence of cultural paradigms and axiological programming or because of their own personal life narrative. There are many elements that support the idea that the five interviewees have tried to offer the most trustworthy account of their cases, trying not to contaminate these with their subjective world, but have tried instead to talk from a professional and emotionally detached standpoint. In many instances, such is the nature of qualitative research; their personalities emerged in the discourse. NPEX1 showed a passion for policing, as well as a fast-paced, “down to earth” way of expressing it. NPEX2 was more ironical and even humorous at certain points, NPEX3 tried to be as detached as possible, PSEX was very critical of societal values and GCEX used a professional yet “everymanish” and critical approach.

## **Chapter 6: Integrated Discussion and Validation of SAT-RI Model**

The online survey and the interview data were analysed and discussed in the two previous chapters. This next chapter is dedicated to integrating the above quantitative and qualitative and quantitative strands; this being the crux of the present researcher's mixed methods approach. As it was indicated in the epistemology section (in the Methodology chapter), the epistemological approach was to be essentially interpretivistic, given that the research relates to the fields of perceptions (for example, the morality of others and perceptions of criminal identity).

The survey and interview methods complement each other and were chosen in order to establish and explore the theoretical design, as has been discussed. The mixed methods used in the study are not only a mere sum of opposing approaches (quantitative and qualitative). Rather, the different methods were used to help answer distinct but interlinked research questions. The online survey was intended to enable the present researcher to identify the role of self-control, morality and neutralisation in cybercrime causation.

The interviews were designed to further understand the use of neutralisations by cybercrime offenders, as well as to inform several social and cultural issues that transcend the theory (yet permeate it). The use of these interviews adds layers of depth to the formulation of the SAT-RI, as cybercrime involves a number of psychosocial issues that cannot be addressed only from a statistical or quantitative perspective. These social and psychological issues offer a discourse on society that will be analysed in this chapter: a discourse on hypermodernity and liquid modernity, on societal changes and new cultural paradigms. Finally, an adjusted theoretical

model is presented and defined in this chapter, along with its constituent elements. The adjusted theoretical model represents the essence of this thesis, which aimed to developing SAT for the explanation of cybercrime.

Issues of gender, identity, sexuality and pornography are discussed in this chapter as they proved to be recurrent themes during the data analysis and academic literature. Revisiting the cyborg discourse presented in the literature review chapter is also necessary. The idea of mankind influencing the machine and the machine influencing mankind, and both influencing and being influenced by society, nurturing an evolutionist circle, is paramount to understanding why cybercrime has become the widespread phenomenon it is now. The rapport forged with the machine (essentially the internet) is also absolutely necessary in order to understand the perceptions from the online survey and the construction of cybercrime and cybercriminals by law enforcement agents who were interviewed.

## **6.1. Reformulation of SAT-RI Model**

### **6.1.1. Answering research questions**

After the online survey and the law enforcement agents' interviews analysis, the SAT-RI model had to be re-structured, into a sequential model, instead of a simultaneous model (one where the variables converged at the same time). The research questions have been answered in the following manner:

*RQ1. What is the role of self-control in cybercrime causation?*

The influence of different levels of self-control on the commission of cybercrime was found to be very important in the present study. Self-control has been measured using a 24 item scale comprising six sub-scale variables (impulsivity, simple tasks, risk-seeking, egotism, physical activities and temper), which represented the elements of self-control following Gottfredson and Hirschi (1990). According to Gottfredson and Hirschi, individuals with low self-control are more prone to the commission of crime as they do not have the capacity to postpone immediate satisfaction. This is due to the fact than individuals with low self-control tend (as theorised by Gottfredson and Hirschi (1990, pp. 89-91) to be individuals oriented to the short-term without a liking for carrying out complex tasks, very keen on taking unnecessary risks and on physical tasks rather than mental ones. Also these individuals are self-cantered and impulsive, and lack the ability to manage conflict. The 24 items also were computed into a new scale variable called “self-control”, produced by aggregating all the answers from the scale. This was done as recommended by Grasmick et al. (1993), who understood self-control as a “coalescent” and unidimensional trait. Also, a dichotomous variable was computed in order to divide respondents into membership of two different groups: those with high and those with low levels of self-control.

Statistically, self-control was compared, using T-Tests, ANOVAs and *chi-squared* tests, to the other variables that formed the SAT-RI (engagement, morality and neutralisation). The self-control variables (the interval variable and the dichotomous high and low variable) were statistically relevant in terms of perceptions of morality and engagement in cybercrime activities. In other words, those with higher levels of self-control were (usually) less prone to the commission of cybercrimes and understood cybercrimes as more morally wrong. This association was broken in respect of some vignettes, which acted as “outliers” (essentially



sexting, Wi-Fi Stealing and Illegal Downloading that are subject to a special discussion in this chapter).

Comparison between self-control and neutralisation techniques produced different results. ANOVAs demonstrated that people with higher self-control were more likely to choose the “this is not justifiable” technique. (This answer was introduced into the survey questionnaire as a “non-neutralisation technique”.) However, self-control was not associated with any other neutralisation technique.

*RQ2. What is the role of personal propensity (morality and engagement) in cybercrime causation?*

SAT-RI theory is an updating of Wikström’s SAT theory for the Internet environment. The core of Wikström’s theory can be found in the “formula: propensity x exposure” to criminogenic setting equals crime causation. Propensity and exposure are based on moral norms: the moral norms of the individual and the moral norms inherent to the environment, including its deterrent capabilities. Perceptions of morality were introduced into the questionnaire following research by Schoepfer and Piquero (2006) modelled as different vignettes for participants to rate. Another variable - “engagement” - was created and introduced into the survey to assess the likelihood a participants would participate in the acts depicted in the scenarios. The reason for using two different variables to measure the same concept (propensity) was related to the projective nature of the questionnaire, given that opposing sets of questions tried to avoid “social desirability bias”. Results showed very good correlations between pairs of scenarios - respondents who understood one scenario as morally wrong were less likely to be involved in it. Also, a trend emerged whereby participants tended to rate the

majority of scenarios as morally reproachable and their engagement in them as very unlikely. They formed what was called the “morality precipice” due to the steep shape of the distributions (modes were usually either 0 or 10, the two extremes of the Likert scale).

However, this symmetry was broken from time to time, when respondents were faced with “outlier vignettes” (Illegal Downloading, Sexting and Wi-Fi Stealing). One of these vignettes was Sexting, that was rated as “morally lukewarm”) but would not engage in them. At the very same time, statistically significant results were obtained when comparing the morality and engagement variables with the neutralisation techniques.

In relation to the interview data, several types of moral structures emerged: professional cyberoffenders who understood their trade as sustenance and online child sex offenders. The latter processed their cyberoffending activities through cognitive distortions. In addition, a distinction between different professionals emerged: cyberfraudsters and hackers. Cyberfraudsters were professionals who had a disproportionate liking for economic gain. Hackers, on the other hand, had a more liquid morality, shifting between constructions of good and evil.

*RQ3. What is the role of neutralisation techniques in cybercrime causation?*

Analysis of the survey data showed that the function of neutralisation techniques was to shield the offender against moral repulse and facilitate the hypothetical commission of cybercriminal acts. The survey offered eight neutralisation choices. These choices stemmed from classical

neutralisation theory (Sykes & Matza, 1957) and current studies on cybercrime and neutralisation (Moore, 2011).

Denial of crime (“I haven’t done anything wrong”), denial of victim (“It’s the victim’s fault”) and denial of responsibility (“It’s not my fault” and “I didn’t have any other choice”) seemed to be very effective and widely picked by participants.

It was also evident from the interviews that neutralisation techniques played a role in cybercrime causation. For example, some child sex offenders joined an online community, of likeminded individuals, in which they were offered solace and justification for their behaviour . Simultaneously, several cognitive distortions seemed to be at work, like understanding child sexual agency and blaming infants for sexual approaches. Law enforcement agents indicated that other criminals used other neutralisation techniques, such as, “I haven’t done anything wrong” and “this is not a crime”. One of the core issues that stemmed from the interviews is whether, or not, offenders lie, tell the truth or are perceived as lying or telling the truth by police officers. Police officers were cautious as to why cybercriminals might have used a neutralisation technique, but they were able to identify and describe the techniques accurately.

*RQ4. What is the relationship between morality, self-control and neutralisation techniques in cybercrime causation?*

It has been demonstrated above that propensity (morality and engagement) and neutralisations do not occur simultaneously, mediated by self-control. It is worth re-stating

that the initial theoretical model considered this relationship (neutralisation techniques and propensity) to be of co-causality. For example, an individual with high cybercrime propensity and a sufficient catalogue of neutralisation techniques starts to use the internet. He is likely to commit a cybercrime if his self-control is low at that moment. Neutralisation, propensity, engagement and self-control were theorized by the researcher to converge at a very precise moment in relation to the internet and work together as coadjutants thereby causing cybercrime. This can be seen in Figure 6, in the literature review chapter, as the “propensity x exposure x neutralisation formula”.

*RQ5. What are the general population's views and attitudes towards cybercrime?*

The majority of respondents taking part in the online survey did not show propensity towards the commission of cybercrimes. In fact, there was a general feeling of moral reproachability towards those crimes that involved violence, psychological abuse and abuse of trust (for example, Cyberbullying and Cyberfraud). Crimes with a sexual content, such as Revenge Porn and Cyberstalking, were found to be especially repulsive. On the other hand, Sexting was not understood as wrong by the generality, maybe because it involved what was, for participants who lived in Spain - who comprised the large bulk of the sample - non-illegal practices (where this involved sending pictures). Also, one might argue that as some aspects of sexuality are sensitive social issues, the “social desirability bias” and the “correspondence bias” may have directed the respondents towards what was deemed to be acceptable or right by them or the researcher.

By contrast, Illegal Downloading and Wi-Fi Stealing (even though they are illegal in Spanish legislation) were not varnished with negative connotations. This might be due to the wide spread use of neutralisation techniques, but also because of a change in social paradigms precipitated by digital technologies. The notions of downloading music and films from the internet and the “necessity” to connect to the internet at any cost, as if it were a human right, seemed, among the survey sample, to be part of current generational trends. Several studies on neutralisation techniques and the music industry were discussed in the literature review (Higgins et al, 2011; Hinduja, 2007; Ingram & Hinduja, 2008; Moore, 2011; Moore & McMullan, 2009).

Police officers constructed the cybercriminal in various ways. For them, some of these offenders are vicious fraudsters looking for economic gain at any cost and who are borderline psychopathic in their profiles. Others are child sexual abusers (some of whom assault very young children) who have a convulsed psychological makeup and who even regarded as “monsters” by other child abusers. A third group of cybercriminals is constructed as more amicable, intelligent ‘riffraff’ without a choice; hackers with a hunger for knowledge; virus creators who want only to earn money the easy way; or even cyberactivists motivated by personal grudges. To this third group, police officers demonstrated an empathic proximity (yet somewhat paternalistic). The other groups are described in a more vitriolic manner or simply with professional detachment.

*RQ6. How do law enforcement agents investigate and tackle the issue of cybercrime and cybercriminals?*

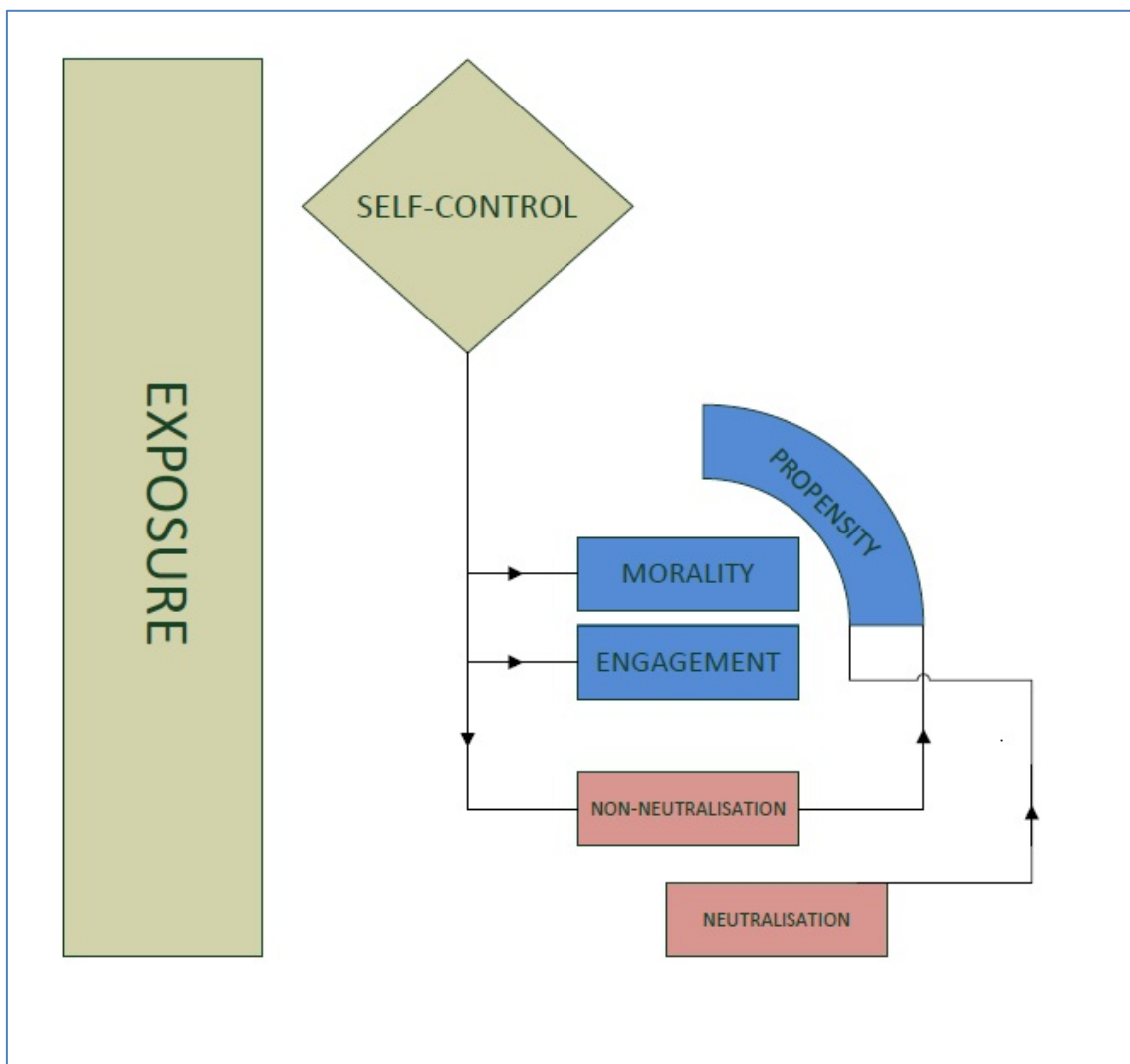
The Spanish law enforcement agents demonstrated a very high degree of specialisation in their work and knowledge, with considerable knowledge of psychology, criminology and law. They do not seem to adhere to British police culture as described by Reiner (2010). This might be due to their: generally ascribing to different moral values than their British counterparts; being members of specific Spanish police corps (Cuerpo Nacional de Policía, Guardia Civil and the private sector), which may have had their own “sub-cultures”; or being higher ranking officers who had acquired specialised knowledge and street experience (which distanced them from lower ranking agents). Spanish “cybercops” and “cybercop culture” call for more research and investigation on their understanding of policing and crime. It was difficult to separate what constituted a personal account, a professional account, what was an institutional directive and what was informed by academic literature. During and after the analysis and discussion of the interview data, enough caution was exerted in order to being able to differentiate between these perspectives, thanks to the discourse analysis. There was evidence to indicate that officers were, in essence, able to provide professional accounts. Yet, there is a reasonable possibility that the accounts were to some extent a bricolage of personal opinion, professional experience, institutional mandate and academic training.

In terms of investigation and tackling cybercrime, law enforcement agents demonstrated good technical knowledge, social skills, and the ability to navigate the internet and social networks with ease. They were also very creative and extremely determined. However, and as indicated before, a cultural study on Spanish police would be extremely valuable.

### 6.1.2. The SAT-RI “circuit of cybercrime” based upon the online survey

The relationship between the SAT-RI variables has proven to be more complex and layered. Figure 22 presents a re-formulation of the SAT-RI triangle, now understood as a sequence that will be named metaphorically: “The circuit of cybercrime”.

Figure 22. The SAT-RI circuit of cybercrime based upon online survey data



Once the data from the online survey was analysed, the following conclusions were drawn. Self-control modulates cyber-crime propensity, as generally those with high self-control do not engage in cybercriminal acts and rate them as morally wrong (with some exceptions, such as Wi-Fi Stealing, Illegal Downloading or Sexting). In other words, self-control tends to affect graver cybercrimes.

Self-control also affects the pick the unjustified neutralisation techniques. Yet self-control did not seem to impact upon the use of other neutralisation techniques. Higher (and especially high) self-control is, therefore, an indication of lesser tendencies towards cybercrime in general; as individuals with high self-control tend not to show crime propensity or the necessity to justify their anti-normative behaviour.

According to Figure 22, the first step towards the commission to cybercrime would be the lack of enough self-control, leading to higher cybercrime propensity and less capacity to opt out in terms of neutralisations.

The second key variable to consider is non-neutralisations (the “Unjustifiable” answers). It was necessary (after analysis of the results stemming from the statistical analysis of the survey data) to create two divisions in the reformulated SAT-RI mode: the “Unjustifiable” neutralisations (lack of neutralisations) and all the other ones that would include the use of any neutralisation technique. The resulting opposing concepts are “non-neutralisations” (unjustifiable) and neutralisations . As indicated above, non-neutralisations are indeed affected by self-control. Also, non-neutralisations affect propensity, given that individuals who tend to see cybercrimes as unjustifiable have demonstrated lesser cybercrime propensity (in terms of



higher morality means and lesser engagement means). These findings create the image of a closed circuit of sorts, as self-control affects propensity and non-neutralisation, and non-neutralisation affects propensity. The circuit imagery captures the profound redesign of numerous psycho-social paradigms produced by the embedment of technology into the fabric of human existence.

According to Figure 22, the second step in the commission of cybercrime is the lack of non-neutralisations, which can affect cybercrime propensity. These two mentioned steps are closely-linked and feed into each other.

Finally, the last key variable to consider is neutralisation. These neutralisation techniques when used effectively (and this solely depends on the type of cybercrime to which they are applied), have the capacity to enhance cybercrime propensity by dulcifying the perceptions of morality and by boosting the engagement means. Individuals who apply an efficient neutralisation technique to a cybercrime would regard it as less morally despicable and would feel more disposed to commit such a crime.

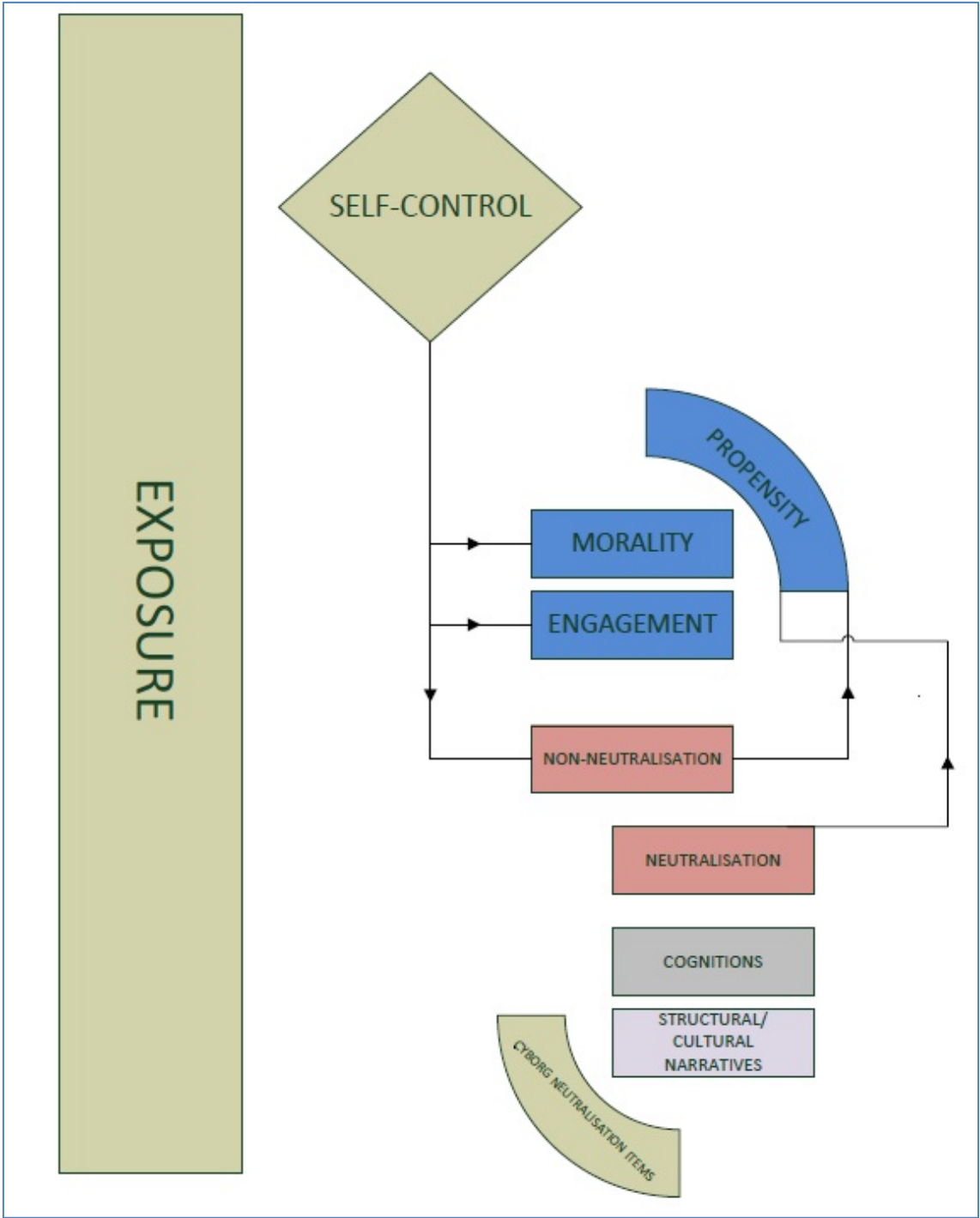
According to Figure 22, the third key step towards the commission of cybercrime is presenting an adequate neutralisation technique in order to boost cybercrime propensity. As shown in the findings from the online survey, some techniques might be effective for a specific type of cybercrime, but not any or not all are effective for any or all cybercrimes.

The new formulation of the SAT- RI as a “cybercrime circuit”, working sequentially instead of absolutely simultaneously (as initially proposed) demonstrates implications in terms of cybercrime prevention. Prevention programmes should be designed in order to act over different stages and layers of the “circuitry”, depending whether either the flux of neutralisation or the flux of propensity are to be managed.

### **6.1.3. The SAT-RI “circuit of cybercrime” after mixed methods integration**

The circuit depicted in Figure 23 follows on from the integration of the online survey and the law enforcement agents’ interview data. The interview data adds more depth to the different stages of the circuitry by adding the elements of “cognitive distortions” and “structural/cultural narratives” that are part of what will be referred to as “Cyborg Neutralisation Items (CNIs)”. These cyborg items are collective neutralisation techniques stemming from the rearrangement of social structures brought about by digital technologies. Structural and cultural narratives relate to the idea of the “culture of free”, “culture of security”, “capitalistic drive” (the so-called “capitalistic critique”) and even notions of gender (for example, the neutralisation technique mentioned in the interview data as “robust heterosexual identity”). “Cognitive distortions” refer to the ones used by online child sex abusers (“the paedophile community”), but they could be applied to other behaviours occurring on the internet.

Figure 23. The complete SAT-RI circuit of cybercrime



## **6.2. The Cyborg Construct in the Reformulated Theoretical Model**

### **6.2.1. Cyborg theory redux**

It is necessary to revisit the idea of the cyborg that was presented in the literature review chapter. The crucial elaboration of the concept stems from Haraway's seminal work and her conception of such an entity as a postmodern, feminist milestone; and cultural, anthropological and political metaphor. The author indicates that "A cyborg is a cybernetic organism, a hybrid of machine and organism, a creature of social reality as well as a creature of fiction" (Haraway, 1991, p. 149). She further contends that it is "a creature in a post-gender world" (1991, p. 150) and she then refers to the three "crucial breakdowns" that have enabled the birth of the construct: The breach of "boundary between human and animal" (1991, p. 152), the distinction "between animal-human (organism) and machine" (1991, p. 152) and the imprecision of the "boundary between physical and non-physical" (1991, p. 152). In relation to the referred blurring between human and machine she argues that:

Late twentieth-century machines have made thoroughly ambiguous the difference between natural and artificial, mind and body, self-developing and externally designed, and many other distinctions that used to apply to organisms and machines. Our machines are disturbingly lively, and we ourselves frighteningly inert. Technological determination is only one ideological space opened up by the reconceptions of machine and organism as coded texts through which we engage in the play of writing and reading the world. (Haraway, 1991, p. 152)

Haraway's work has generated considerable academic attention. This might be due to its obscure, and somewhat allegorical and figurative nature, and its capacity to lyrically discuss

the role of women in the “dictatorship” of masculinity, science and technology, or politics and the postmodern blur of dichotomies. Wilson (2009) indicates that the cyborg is “a material-semiotic entity”, a “figuration” and a “narrative device” (pp. 501-502). In addition, Kuni (2007) discusses several cyberfeminist approaches to art and language, and the idea of cyborg writing, based on the conception of language as a virus. All these ideas seem to demonstrate that the cyborg construct serves as a metaphor embedded in the sympathetic relationships that many human constructions forge between each other, but also with technology and biology.

As to the key ideas permeating the cyborg concept, we must understand that essential consequences of the connections between humans and tools reviewed by academic literature. The cyborg results in: “augmentation”, (Wells, 2014, p. 11; citing also Clynes & Kline, 1960), and “embodiment” and “hermeneutical” (Vicini & Brazal, 2015, p. 151). Augmentation refers possibilities brought by the cyborg, not only in enhancing bodily functions, but also in changing and jumpstarting social and cultural processes (Wells, 2014, p. 11); embodiment to the tool becoming part of the users physique and/or identity; and hermeneutical to the idea of the tool becoming an extension of the self (Vicini & Brazal, 2015, p. 151).

Vicini and Brazal (2015) provide another perspective on the cyborg, constructing it in theological terms, comparing it with the “(Cyber-) Body of Christ”. By following the ideas of embodiment, sacramentality, difference and solidarity, they offer a Christian and ethical reading of the term “cyborg” (pp. 161-164). These authors also touch upon the concepts of posthumanism and transhumanism. Transhumanism refers to the idea that “technology needs to be used to transform the human body and human nature” (p. 155), whereas posthumanism represents the idea of moving forward (socially and individually) into the next step of evolution

by using technical ability and human will (p. 155). These two concepts are connected, with transhumanism being the “midwife” and delivering posthuman civilisation. Hayles (2010) explains that “just as the posthuman need not be antihuman, so it also need not be apocalyptic” (p. 22). She believes that posthumanism will come to mark the end of current conceptions of humanity, which are based upon inequality and the privileges of a powerful over-class. Technology is thus understood as empowering and liberating for humanity, yet not unburdened of certain perils as this present thesis aims to demonstrate. Wells (2014) contends that “the cyborg concept simply (perhaps ironically) describes us as we already are, as we have been for some time, and as we are likely to continue” (p.10). Humanity has forged deep relationships with machines through history, some of them with drastic and positive evolutionary consequences, in cultural, biological, psychological, sexual and social dimensions. All in all, the internet has had a more profound impact, and upon many different aspects of human existence, than any other artifact or tool ever developed. However, the idea of elevation and transcendence seems to be emphasized in the cyborg theory, but the human/machine interface could also generate deviant and non-normative behaviours. Connor, Coombes, and Morgan (2015), for example, relate Haraway’s metaphorical cyborg concept with anorexia sites. They refer to how anorexic girls’ posts on pro-anorexia issues (in terms of content and structure) mirrored their bodily states and how their body metaphorically expressed itself through the blogs, for instance, by “feasting on information” (p. 239), “starving” (p. 239) or a necessity for “connectivity” (p. 240). The girls’ relationship with their blogs was a relationship that implied, essentially, embodiment but also hermeneutics (as anorexia is related to bodily perceptions). These girls gave tips on how to be “properly” anorexic, they even offered nutritional advice and they supported each other in their “community”.

Going back to the technological and social discourse, Katz and Aakhus (2002) have developed the term *Apparatgeist* “the spirit of the machine that influences both the designs of the technology as well as the initial and subsequent significance accorded them by users, non-users and anti-users” (p. 305). Lever-Mazzuto (2012) summarises the theory, explaining that it “examines one’s relationship with his or her technology, as well as the relationship that the two have with society” (p. 83) and that “the essence of Apparatgeist Theory: norms for technology use are socially constructed” (p. 83). The thesis proposed by Katz and Aakhus is not dissimilar to the cyborg construct; however it is more focused on the social role and social consequences of mobile phones use. They refer to the idea of “perpetual contact” (Katz & Aakhus, 2002). This is extremely relevant as it refers to the impact of mobile phones and other digital technology in social decision-making, as well as the way this technology has penetrated the sphere of the intimate. More importantly, it refers to how the use and design of digital technologies follow normalised patterns all around the globe. According to the authors, technologies affect the entire world in a similar fashion. They also highlight the anxiety that the absence of contact produces in a networked world. In relation to this last point, Castells (2010) explains the characteristics of the networked society (pp .70-76). Some of the features of this society are the “pervasiveness of effects of new technologies” (p.70) - meaning that technology shapes all the facets of our existence - “the networking logic” and “flexibility” (pp. 70-71). The system is organic and must grow, connect, adapt and change; creating higher structures or changing them. The idea of “convergence” (p.71) becomes extremely relevant, here, whereby different technologies or systems tend to integrate with one another. Castells reflects upon the idea of convergence by stating “the information technology paradigm does not evolve towards its closure as a system, but towards its openness as a multi-edged network” (pp. 75-76). He then moves onto the discourse concerning technological change by adding that technology is a force “under the current technological paradigm that penetrates the core of life and mind” (p. 76). Humans have become intertwined with technologies in

irredeemable ways, either under the cyborg fusion, which Haraway explains metaphorically, creating new entities that do not (and should not) abide by antiquated rules of science, biology and technology; or according to the *Apparatgeist*, where the rules of the machines define society and society defines the rule of the machines, or as an organic ever-growing system envisaged by Castells: a system that is shaped by the nature of networking machines. That system is always changing, evolving and in perpetual necessity of connectivity and integration.

All of the abovementioned contentions are extremely relevant in light of the findings of the study at hand. The survey and the interview data have brought to the forefront important societal issues that need to be addressed - issues that relate to the shifts in social paradigms brought about by the internet and the becoming cyborg. The reason for dealing with these matters, once again, in this penultimate chapter is to produce a revised SAT-RI model that includes new elements that emerged during the analysis of data. The essence of the literature review, in Chapter 2, was to present and assemble SAT-RI, to put together the general theoretical drawbacks in the elaboration of cybercrime, to give examples of cybercrime and to address the sociological issues relating to the permeating of new technologies into social and personal lives. This permeation was quite conspicuous in both the online survey (for example, the acceptability of stealing W-Fi signal and the illegal downloading of movies) and the law enforcement agents interviews interview data (for example, the creation of an online paedophile community and the sense of security that criminals have on the internet). This chapter, which tries to bring together and intertwine both sets of findings, is the forum in which the cyborg discourse will be deepened. The present researcher has also decided that the ideas relating to the cyborg construct should be included in the reformulation of the model ("the circuit of cybercrime"), as they were not present in the original model and they can help explain the etiology of cybercrimes. The discourse of how structural forces (market forces and



gender constructions serve as good examples) guide, model or affect the rapport with the internet (and vice-versa) has become integrated in the theoretical model as the findings indicated that they played a role in the commission of cybercriminal acts.

### **6.2.2. Cyborg neutralisation items**

Different narratives seemed to emerge following analysis of the interview data. None of these narratives had a clear adscription to the theoretical structure of neutralisation techniques or cognitive distortions. These narratives referred to the broader socio-cultural Spanish structure, rather than a personal introspection on the part of offenders. Dissimilar as these narratives might appear to be, they do have a profound connection to neutralisation techniques, as both stem from patterns of normalised morality and bourgeoisie morality (the social), and they serve to personally justify the crime or cyber-crime (the anti-social). The essence of traditional neutralisation technique theory is that the delinquent still “clings” to dominant supra-personal moral normativity: “he would appear to recognize the moral validity of the dominant normative system in many instances (Sykes & Matza 1957, p. 665)” and needs to justify his/her acts by resorting to that system.

In the case of the proposed “Cyborg Neutralisation Items (CNIs)” a different process occurs (yet one not entirely disconnected from the traditional neutralisation process). Stemming from the different accounts contained within the interviews (and it must be noted that all of them reflect upon Spanish society), several new codes emerged, “ex post” and unrelated to all the neutralisation techniques discussed in earlier chapters. What was common to all of these accounts was that they represented a social critique, explicit or implicit, which reflected how

these police officers understood several social issues. At the same time, those Cyborg Neutralisation Items (CNIs) can be implicitly found in the online survey data. These CNIs have been theorised by the researcher after the data analysis and their definitions are offered in this chapter.

It is important to note that these CNIs are theorised when juxtaposing the abovementioned accounts to current sociological or anthropological literature and that they suffer from the general limitations of the interview data. These CNIs are born from accounts narrated by police officers, and are therefore inherently subjective and possibly influenced by all the facets of police culture (Reiner, 2010). At the same time, it must be recognised that one of the major conclusions from the analysis of police culture – based upon the sample of Spanish cyber-police - was that cyberpolice officers seemed to depart from the seven key elements of Reiner's police culture (2010, p. 117).

Cyborg Neutralisation Items (CNIs) are defined as:

Explicit or implicit socio-cultural compulsions and/or narratives that originate in the intersections between the internet user, the internet in itself (or any aspect of information and communications technologies) and structural constructs (like extreme capitalism or gender semiotics), and serve to drive the user to the commission of cybercrimes and enable collective or personal justification of these crimes.

The CNIs that will be discussed here are “a capitalistic critique/drive” implicitly stated in many of the accounts and “the culture of free” and “the culture of security”.

#### **6.2.2.1.     *A capitalistic critique/drive***

This item is presented as a critique and it also works as a neutralisator by supposing a social drive that directs the actions of many individuals involved in cybercrime: an external force driving the commission of cyber-crime like a cultural tropism. This CNI also relates to other notions obliquely related to extreme capitalistic societies, such as narcissism and the commodification of sexuality.

Briggs (2013), talks about the blinding and binding powers of extreme capitalism in his studies of British holidaymakers in Spain, engaging in conducts of excess, consumption, risk and deviancy:

They [the sample] are as much a by-product of an ideological social conditioning of being over a period of time as they are drawn into excessive consumption, deviance and risk taking by the powerful corporations, commercial entrepreneurs and tourist companies/organisations. (p. 45)

He also suggests, in relation to this group of holidaymakers, that “a kind of emic and reflexive evaluation of the self takes place as they become unhinged from everyday home life” (p. 46). The aforementioned reflections refer to British holidaymakers in Spain, and to their constructions and de-constructions of the self, based on their creation of the ideal “extreme” holiday as programmed by capitalistic “software”. From this, Briggs develops the idea of “unfreedom” (Briggs, 2013a, 2013b). In relation to the present study, one could ask whether the above holidaymakers - reshaping their identities and actions according to extreme capitalism – represent society more generally: the cyborg constructs travelling throughout and

by the internet in a perpetual anthropological holiday. What if the psychic rapport with the machine - which leads to cybercrime- is woven by threads of extreme capitalism?

In a similar fashion, Lipovetsky (2005) develops the idea of hypermodernity, a time of hyperbolic excesses following postmodernity. In this hypermodern epoch “hypercapitalism is accompanied by its double: a detached hyperindividualism” (p. 33). This pathological necessity to anchor the present against the anxieties of the blurring future creates a “civilization of ephemerality” (p. 39). In such a civilization, consumption, media and fashion take center-stage:

The world of consumption and mass-communication appears like a waking dream, a world of seduction and ceaseless movement, whose model is none other than the system of fashion. (p. 36)

At the same time, “in the functional universe of technology, dysfunctional behaviour is on the increase” (p. 33). Lipovetsky’s themes are very relevant to the present work. This is because these themes enable a critical connection to be made between consumerism and technology, relating to many of the emergent narratives found in the law enforcement agents’ interview data, and the narratives underpinning some of the quantitative findings. Parallel ideas are found in the discourse by Bauman (2000) on “liquid modernity”, where he addresses the concept of individualism and its profound links to consumerism (and vice-versa). Bauman (2000) discards the idea of “needs”, and focuses on the creation and production of “desire” (pp. 74-75). Thus, “consumers guided by desire must be ‘produced’, ever anew, and at high cost” (p. 75).

The abovementioned ideas of desire, excess, extreme capitalism, engineered necessity and hyper-consumption seem to be found in the accounts coded as “a capitalistic drive”. A very

good example of this is found in C17: “Why are you asking for only 2,500 €? It’s because I wanted to buy a bicycle” (NPEX2, C17<sup>lxxv</sup>).

In C17, a 16 year old minor when trying to extract a ransom from a powerful company and asked for exactly 2,500 €. NPEX2 explained that this boy confessed that he had done this before albiet in exchange for a smart-phone. (The offender lived in deprived northern Spanish village.) Other relevant accounts in terms of a capitalistic critique are those found in GCEX and NPEX3’s depiction of cases C2, C18 and C19.

GCEX explained how, in C2, The Guardia Civil investigated a group of minors who were offering sexual services, via a social network. The children involved ranged in age from 10 to 15 years. The minors sexually penetrated male adults and allowed male adults to touch them or perform fellatio on them in exchange for small amounts of money and “desirable” goods, such as mobile phones and game consoles. These minors were recruited into these freelance activities by other minors, already involved in these practices, who had been boasting about their new possessions. GCEX’s involvement in C2 led him to reflect on the importance of sexuality for young children: “the value of maintaining a sexual relationship... I mean, a boy it’s not very clear on how much it is worth or the cost of it” (GCEX, C2<sup>lxxvi</sup>). At the very same time, those children were able to maintain their hegemonic heterosexual identity and status by resorting to the “robust heterosexual identity” neutralisation. Hyperconsumption, therefore, is able to “corrupt innocence” leading children into sexual activity with male adults and even truncate their own heterosexuality. Mercer (2012) reflects upon straight performers in gay pornography and the idea of “straight men for consumption as homoerotic objects” (p. 540). It must be noted that he is talking about consenting adults in pornographic films fulfilling contractual obligations, as opposed to children offering themselves sexually for adults in contravention of

legal norms. What is interesting about Mercer's discourse, though, is that sexuality and/or sexual orientation can become products for massive consumption, via the internet, even if endangering heterosexual normativity. He talks about "alibis" (Mercer, 2012, p. 540), which are cultural or artistic neutralisation techniques that serve to justify heterosexual identity. These alibis are "the financial alibi" (p. 541), "the amoral alibi" (p. 542) and "the exploratory alibi" (p. 544).

In contrast, NPEX1 discussed how cyberfraudsters are criminals with a "disproportionate motivation for economic gain" (NPEX1, C10 and C11<sup>lxxvii</sup>) when presenting a profile of the cyberfraudster. The wording of the explanations in his discourse on cyberfraudsters is almost identical (*ánimo desmedido de lucro* and *ánimo de lucro desmedido*; only changing the position of the adjective disproportionate) in these two cases as NPEX1 had interiorised that idea as a police mantra; one that might have stemmed from the criminological literature or from police his police education. It should be noted that these profiles of cyberfraudsters were drafted by NPEX1 (as he was the first law enforcement agent to be in contact with the offenders when they came to be investigated) and not by the researcher. NPEX 1 stated, in respect of C11, that "If I want to earn money and have no scruple<sup>lxxviii</sup>" you can resort to fraud. In NPEX1's interview the word "*dinero*" (money) was mentioned 66 times and in NPEX2's interview 28 times (both Police officers focused on several matters relating to online fraud, hacking and computer virus design). PSEX also talked about money when explaining C7, a case of industrial espionage that took place in the private sector; where employees disclosed information to other companies in exchange for money "everything is for sale, nowadays absolutely everything is for sale" (PSEX, C7<sup>lxxix</sup>).

In a word cloud (Figure 27) generated through NVivo 10, depicting the 20 most frequent words in all of the interviews, “dinero” (money) was cited most often, even more than internet or “ordenadores” (computers). “Empresa” and “empresas” (company and companies) were also referred to quite frequently. “Pago” (payment) appears amongst the 20 most repeated words as well. References to capitalistic structures are, therefore, recurrent in the interviews.

Figure 24. Interview word cloud



NPEX3 made the following criminological reflection upon the idea of women involved in online paedophile rings and the production of child pornography as a business:

Yes, yes, there are more and more women in relation to this and the majority of women we had at the beginning was evidently that were into these matters of child pornography within the sphere of prostitution, I mean, as another way of earning money. But now, we are also seeing that, effectively, there is a group of people that are women and are paedophiles and that are pederasts. (NPEX3, C18<sup>box</sup>)

And,

There is plenty of child pornography production that only looks for economic gain, when we talk about organized crime, the recruiting of children, the creation of webs, the money laundering proceeding from the sales of child pornography ... there are merely economic interests because it generates plenty of benefit. (NPEX3, C18<sup>lxxxj</sup>)

NPEX3 assumed the existence of two types of individual involved in online child pornography: those who subject to powerful cognitive distortions, who are driven by paedophile interests; and those who comprise persons involved in organised crime, the production of child pornography or women involved in prostitution, who are motivated by an economic considerations. NPEX3 envisions some of these networks as businesses, satisfying the demands of a globalized networked world. Thus, according to NPEX3, crime can easily follow the diktats of market forces and extreme capitalism. From a feminist perspective, Harrison warns that “some feminist and profeminist writers have consequently argued that it is spurious to distinguish between adult and child pornography” (2006, p. 370). Online pornography will be discussed in more detail in below, and feminist perspectives will again be utilised. It is important to note here, though, that child pornography and pornography can be understood as forms of social gendered violence against women and children, reproductive of structural inequalities (Harrison, 2006; Tsatsou, 2012, p. 520). Thus, women committing child sexual offences and producing child pornography (for economic purposes) represents a very complex issue, a possible feminist contradiction. That said, the proportion of child sex offenders who are female small: “Offenders were all white, and 18 of the 19 offenders were male. The one female was offending in conjunction with a male offender” (CEOP, 2013b, p. 20). Gannon and Alleyne (2013) produced a meta-analysis of cognitive distortions in female sexual abusers and



commented on the small body of literature available and judged this to be a major limitation of their review (p. 76).

In relation to the online survey data, this item - economic drive as a CNI- does not seem to be clearly or implicitly identified. As mentioned previously, the majority of the sample was clearly repulsed by cybercriminal acts. The only cybercrimes that were commonly seen as acceptable were Wi-Fi Stealing and Illegal Downloading. Sexting was more complex in terms of acceptance. The reason behind the blatant acceptance of cybercriminal and illegal activities may be that they are embedded in social practices that are not considered cybercriminal (the downloading of movies, for example). In addition, the neutralisation techniques favoured in these vignettes (and which demonstrated high statistical significance in terms of shielding against cyber-criminal propensity) are: "I haven't done anything wrong" (denial of crime), "It's my right" (entitlement) and "I didn't have any other choice". The reason why participants concluded that they had no choice but to steal Wi-Fi, might lie in social expectations or pressures that have elevated access to the internet from being a privilege to the status of a right and necessity, in Western societies. The culture of hyperconsumption could be behind the creation of such a necessity; a "desire" as Bauman has argued (2000, p.73-75). This desire might also explain why individuals are so keen on downloading movies illegally from the internet: "desire becomes its own purpose, and the sole uncontested and unquestionable purpose" (Bauman, 2000, p.73). Following this reasoning, it is not a crime to acquire, by any means, what we are "programmed" to long for: entertainment, culture, movies and music - like intellectual fast-food delivered by cable connections. There is not enough data to support such an interpretation of the survey data and ideally there would have been a follow-up phase to the present research in which qualitative data was obtained from participants on their motivations. However, the literature discussed in this discussion chapter invites the

researcher to consider the incidence of capitalistic structures in the neutralisation of Illegal Downloading and Wi-Fi Stealing.

In order to close this section, a definition of this CNI is offered:

An explicit or implicit socio-cultural compulsion for acquisitiveness (derived from capitalistic constructions) that guides the behaviour of many internet users towards the commission of cybercrime.

#### **6.2.2.2.     *The culture of free***

The culture of free also stems from the overwhelming market forces applied to the cyborg nexus (the individual in contact with the internet and society) and is profoundly connected to the “capitalistic drive”. Once again, Lipovetsky’s (2005) discourse is relevant in that he invites the reader to “witness the mania for consumption” (p. 32). In relation to this “mania for consumption”, PSEX offers a diatribe on current social issues, such as the illegal downloading books and movies. PSEX’s diatribe also refers to other unrelated topics, including infidelity, via WhatsApp, and the generational digital divide. The main question to be asked is whether PSEX is speaking from his experience as a former police officer, and now a private security consultant, or simply as an everyman. Another methodological issue in PSEX’s discourse is that it is not entirely open to triangulation with the survey data, as no other law enforcement agents commented on these particular matters. In spite of these methodological shortcomings, PSEX’s narrative is very relevant. This particular discussion named “PSEX’s diatribe” was generated after at the end of the interview, given that some cases were ruled out as cybercrimes (C5, C6) and other cases were explained briefly.

Jorge: And the topic, for example, of illegal downloading be it movies, [TV] series, music? Do you think people are aware that in that case it could be indeed criminal; do you think people think whether, in some cases, it is moral or immoral? What is your opinion in that regard?

PSEX: My opinion is that people, If they can get something for free. Why are they going to pay for that? (PSEX, no case<sup>lxxxii</sup>)

It must be noted that PSEX is not implying entitlement (entitlement would indicate that they shouldn't pay, as they have a right to it). What cannot really be understood from the narrative is whether he is being ironical, cynical or speaking in a "matter of fact" dialogue.

PSEX continues his diatribe:

Let's say, for example, if I go to the cinema and have to spend 8 € for going to the cinema, If I go and give a simple click, also I am at home, I prepare my pop-corn, my Coke and it's for free... It's not the same, but well, the culture of free, and of what I have obtained that hasn't cost me anything, and well, we are in a [financial] crisis. The crisis deepens and people do not spend that much in... (Emphasis added, no case<sup>lxxxiii</sup>)

He finishes by talking about illegal movie and book downloading, adding "[the offender] doesn't have any knowledge of the whole industry behind copyright, of creator rights" (PSEX, no case<sup>lxxxiv</sup>). His perception is that these practices are not entirely innocuous or innocent, as they may entail damage to the entertainment industry.

The illegal downloading case, in the survey data, engagement -whether respondents would engage in Illegal Downloading - (M=7.71; Mode=10, SD=3.03), whilst perceptions of morality - how morally wrong respondents perceive Illegal Downloading- (M=3.40; Mode=0; SD=2.76).

For the Wi-Fi stealing case, engagement ( $M=7$ ;  $Mode=10$ ;  $SD=3.31$ ) and perceptions of morality ( $M=4.32$ ;  $Mode=5$ ;  $SD=3.02$ ). Looking at the modes, it can be seen how the majority of people would have engaged in Illegal Downloading and Wi-Fi Stealing readily. Also, the majority of respondents rated Illegal Downloading as absolutely moral, and Wi-Fi Stealing as morally correct. Even though the results are similar and coherent (Wi-Fi Stealing and Illegal Downloading), Wi-Fi stealing is, for the sample, less immoral than illegal downloading. The idea of a culture of free could explain these results, especially if considered with the neutralisation techniques ("everyone else is doing it" or "it's my right to do so", for example). Having decided to use an interpretivistic epistemology - based on the idea of a blurring of the frontiers between quantitative and qualitative methodologies (in this mixed methods study) - it is necessary to evaluate this perception. One of the first issues that should be borne in making this evaluation, is that a large proportion of the sample was comprised of "captive audiences" from criminology and law courses. In terms of socio-demographics, an even larger proportion of the sample was made up of university students, lawyers, lecturers and law enforcers. Given these characteristics, the sample should have had a more detailed knowledge of the law (than the general population) that should have led them to understand Wi-Fi Stealing and Illegal Downloading as anti-normative (they are against criminal law, in fact). On the other hand, one could have expected that a sample with said demographic characteristics might have rated any type of anti-normative action as wrong, especially a sample with such high levels of self-control. These were not, however, the findings in the online survey. Only 17.3 % of the survey sample found Illegal Downloading vignette as unjustified - very close to the 18.2 % that found the Wi-Fi Stealing case as unjustified.

It is worth repeating, here, what PSEX said in his interview, in relation to Wi-Fi Stealing:

People do it, but well, really, the commission of said crime is there. Nowadays there is nothing stipulated but we would be stealing or hacking the cost of the Wi-Fi, that amounts for a monthly 30/40 € let's say, that type of crime, well people say: noooooo this is nothing and I do it and sometimes because of the simple fact that I am good at hacking the neighbour's Wi-Fi. (PSEX, no case<sup>lxxxv</sup>)

PSEX emphasised how easy Wi-Fi stealing is, pointing out that there are even mobile applications for facilitating such offences. According to PSEX this behavior has, in a manner of speaking, been socially naturalised . PSEX explained that legislation, in Spain, is to be changed to create a specific offence of Wi-Fi stealing. Up until now, this behavior had to be prosecuted either as a civil wrong or in criminal law by using an analogous approach to “electricity fraud”.

It is important to understand where this sense of normlessness stems from. Having analysed the idea of the culture of free, and the survey and interview data, only two options remain: that the general public is not really aware that they are committing crimes or legal wrongs (for example, administrative or civil wrongs) or that they are aware but it is so intrinsically neutralised by social habit that it has become conventional and non-deviant. It is essential to define by the researcher what is understood as the culture of free and how it works as a CNI:

An explicit or implicit socio-cultural understanding that technological goods and services (software or hardware, including products related to the entertainment and culture industry) are free of charge because of their availability. It also implies that the access and usage of the internet and its fruits are rights or necessities in themselves that should be at anyone's disposal.

#### **6.2.2.3.     *The culture of security***

The culture of security refers to two opposing aspects of computer security obtained from the law enforcement agents' interviews. The first aspect is the absence of a culture of security, which leads to something of a generational divide between younger and older internet users, or the sense of false confidence that some criminals display because of their technical expertise. Both of these states are related to the structure of the internet and the mutating nature of hypermodern (Lipovestky, 2005) and liquid societies (Bauman, 2000), where technological advances happen at an extremely fast pace and are doomed to short-term obsolescence. Bauman (2000) describes this situation with elegance and eloquence when he states that "the insubstantial, instantaneous time of the software world is also an inconsequential time" (p. 118). It is, then, on the internet where changes become much more frequent, difficult to be framed or measured by the devoted user or the mere onlooker. Due to these changes it is very difficult to keep up with computer security.

NPEX1 explained that C12 involved a group of young men posting videos of illegal sport cars races on the internet and the subsequent investigation of an illegal race ring in Spain. Even though this case was deemed as "not entirely a valid cybercrime", because of NPEX1's focus on the investigation of driving offences, there was an element in the case that fell under the umbrella of the cybercrime definition: the posting of content about illegal acts on YouTube.

NPEX1 [Asking Jorge]: Why did he upload the videos, why do you think he uploaded the videos?

Jorge: I have plenty of ideas, but If I tell you...

NPEX1: Is that I haven't really stopped to think. I say, that guy is dumb. The guy is a brat, daddy's boy boasting his feats without thinking in the consequences of his acts, much less thinking that if he's not caught at that moment doing the races, through the internet even less. Then, he doesn't think by a moment that it could be a crime, nor that he is risking anybody's life, nothing. Who does that? A person that is arrogant, boasting about what he has on YouTube channels, uses them for boasting about the money, the cars, all he has, and the people surrounding him, because they were nothing more than poor 18 year-old brats with two brain cells.(NPEX1, C12<sup>lxxxvi</sup>)

The general idea permeating NPEX1's acid explanation of the case is that the capricious youngsters behind the races were not aware of the dangers it represented to them or others. They were also not aware of the dangers of being involved in risky criminal activities and also making it public. Ironically, that publicity, after an exhaustive analysis of all the videos, led NPEX1's team to apprehend all of the offenders. For NPEX1, making the videos available on *YouTube* was an act of narcissism, but also of recklessness. He used the terms "brat", "arrogant", "boast", "daddy's boy"<sup>21</sup> and "dumb", and who possessed "two brain cells", in what seems an act of transforming the protagonist into a pariah by means of irony. NPEX1's street-wise and anti-formal discourse contains a certain black humor ("dumb", "two brain cells", "daddy's boy") that might be mistaken for disdain in certain cases, for example, when explaining how utterly reckless the actions of the offenders were and how they were very unintelligent, bragging individuals. This anti-formality can also be found in NPEX1's swapping the roles of interviewer/interviewee and asking questions to the researcher that serve as a rhetorical invitation. It cannot be really proven that the protagonists of the case did not really know the consequences of their behaviour or were acting out of hyper-narcissistic

---

<sup>21</sup> In fact, the expressions are very similar in English and Spanish as *niño de papa*, means exactly *daddy's boy*

compulsions, yet a certain level of such motivation can be inferred from the act of publicising criminal deeds. Narcissism plays a fundamental role in Lipovetsky's (2005) hypermodernity. Some studies also point to the trait playing an important role in our relationship with the internet, especially when taking into account that plenty of social networks are devoted to the sharing of pictures, videos or statuses of oneself. Fox and Rooney (2015) investigated the relationship between the *The Dark Triad* and trait self-objectification as predictors of men uploading pictures on social networking sites. The Dark Triad refers to the following traits: Machiavellianism, narcissism and psychopathy (Fox & Rooney, 2015). The following results were emerged from Fox and Rooney's study: men that tend to self-objectify and narcissistic men spent more time on social networks, and more narcissistic and psychopathic individuals upload more selfies. However, narcissistic and highly self-objectified men devoted more time to the editing of uploaded pictures. These results might seem obvious, but offer a very interesting insight into the psychology behind social networks (especially those more oriented to photographic images, like Facebook and Instagram). Kasper, Short, and Milam (2014) discovered that "two of the three measures ... indicated that individuals who endorsed higher levels of narcissism also endorsed a greater frequency of internet pornography use" (p. 485).

After the interview with NPEX1's, relating to the C12 case, the present researcher conducted searches on the main offender, on YouTube and Google, using the nickname provided by NPEX1. Several videos were found: in one of them he appeared with several sports cars and in another he was being interviewed for a national TV exposé documentary<sup>22</sup>.

---

<sup>22</sup> The google searches imply he had reached an embryonic level of Internet celebrity, with some of his videos spoofed and news on him, plenty of news; message boards discussions, a twitter account that could be a fake. Even though said information is public and accessible, the primary source was confidential and for ethical reasons it won't be compiled in this work.



NPEX3, when talking about C20 (The Chameleon grooming case), provided a victim's perspective, explaining how adolescent girls were led into believing that they were talking to another girl and then how -and after an exchange of erotic pictures - they were trapped in a web of extortion in which increasingly sexually explicit pictures were demanded from them. According to NPEX3, minor girls were easily manipulated by the groomer into believing that he would send their pictures to others or deactivate their social network's friend's list or webmail accounts. The process of grooming them was as follows:

It's the way of stinging the minors through social networks, they sting them, but then he takes them to other places, I mean he takes them so they facilitate images and videos, be it through Skype or through applications that enable for fast communication. (NPEX3, C20<sup>lxxxvii</sup>)

Although victims were terrified and felt morally degraded by what they had to do, and the intensity and duration of their experience. (NPEX3 revealed that he had investigated some grooming cases where the victim had committed suicide.) The prospect of losing internet access or friend's lists was, according to NPEX3, more frightening for the victims than having to provide pictures or the thought that these would be distributed, and was sufficient to ensure that they abided by the groomer's wishes. In this case, the lack of a culture of security helps to explain how they came to be groomed. This comprised: the use of certain sites and applications by minors (like Skype and social networks); the misinterpretation of the sexual nature of the acts they were obliged to perform and the possible empty threats of deletion of passwords or friend's lists; and essentially their inability to detect dishonesty from their online acquaintances. As discussed above, the pressures of hypermodernity and capitalism, and the lack of proper emotional understanding of sex, enabled children, in some cases, to commodify their own sexuality.

In PSEX's "diatribe", there were several references to a general sense of socio-technological normlessness, with his arguing that "they [minors] are not really aware of that what they are doing is really a crime" (PSEX, no case<sup>lxxxviii</sup>). He said this in relation to minors who published threats or slander on platforms such as social networks and messaging mobile applications. He believed that the problem lay with education:

The thing with education is that there is a great divide, it's called the digital divide, in which you can't instill something into minors without having instilled it previously in elders. (PSEX, no case<sup>lxxxix</sup>)

Adults are not really aware, according to PSEX, of the dangers that the internet and technological devices pose for children in this epoch of ephemerality and immediacy. As an admonishment and maybe in an extremely dramatic tone he used the following allegory:

A father buys a Blackberry for an 11 year-old boy, without knowing that in his hands he has a weapon that can commit, well, the suicide of a girl that is being subject to abuse . (PSEX, no case<sup>xc</sup>)

The continuous change of pace and scenario that occurs on the internet is, following what emerged from C20, C12 and PSEX's diatribe, exemplified by social networks. Social networking platforms thrive in the vertiginous pace of internet development and change. Some networks are more generalist, whilst others are highly specialized, in terms of demographics for example. This may enlarge the digital divide that exists between generations, marked by different use patterns or intensities.

Data provided by Duggan, Ellison, Lampe, Lenhart, and Madden (2015), based on American internet users, revealed that most (87%) Facebook users in 2014 were aged 18-29 years. It is also the most popular site by far, with 71% of American adults using Facebook in 2014. This is

interesting, as although young adults are the predominant Facebook group, it is also widely used by older adults, so there is not an unfathomable divide. Similarly, only 37% of Twitter users are 18-29 years, so the digital divide with older adults is even less stark regarding this social platform. In relation to Instagram, differences are more visible: 53% of 18-29 year olds use Instagram as opposed to only 25% of 30-49 year olds and 11% of 50-68 years. According to Lipsman (2014), Snapchat is the social network that is showing the highest degree of penetration amongst 18-24 years old mobile users. The network is penetrating the market like no other, “trailing only Facebook and Instagram” (Lipsman, 2014). In relation to this, Snapchat.com shares the following information under its advertising tag “Snapchat is the best way to reach 13 to 34 year-olds” (Snapchat, 2015). The following demographic information is displayed on the site: 37% of users are 18 to 24 year-olds, 26 % are 13-17 and 23% are 25-34. Snapchat<sup>23</sup> is a good example of a young social networking site, oriented to a much younger generation than Instagram, Facebook or Twitter, and one which exemplifies the “here and now” orientation of liquid and hypermodern society. Educators, parents and children have different necessities and skills, and their level of internet knowledge might vary. However, data analysed in this present thesis seem to point towards the absence of a widespread culture of security.

In contrast, the culture of security cyborg neutralisation item can be understood from a different perspective: a false sense of security among offenders, who believed that they would not be apprehended because of their wit and skills. As NPEX2 explained, some offenders, such as the ones involved in C14 (the “*Cryptolocker*” case) have “a feeling that they won’t be caught” (NPEX2, C14<sup>xci</sup>), explaining that they were aware of what they were doing, but relied

---

<sup>23</sup> The essence of Snapchat is sharing pictures, video and text that self-destructs in seconds after having been read. According to Snapchat’s Terms of Use “Although these Terms form a proper legal contract—and inevitably read like a proper legal contract—the bulk of them are simply designed to ensure our users have fun (...)Just use common sense: Keep sending awesome Snaps to your friends, and please don’t send Snaps that they don’t want to receive. (Snapchat.com, 2015)

on that sense of protection facilitated in many cases by the architecture of the Internet (anonymity is a clear example of this). NPEX3 went on to say that offenders were aware of what they were doing, but relied on the sense of protection facilitated in many cases by the architecture of the internet (anonymity is a clear example of this). NPEX3 touched upon these themes when explaining the “paedophile community<sup>xclii</sup>”, and how it served to justify and protect offenders psychologically by disseminating several cognitive distortions. NPEX3 was sure that without the internet this “shadow community” would not have been created and then reinforced. This is important, as the existence of the community influences the cognitive schema of child sex abusers.

It is difficult to elaborate, from the survey data, on these ideas of a sense of security or the lack of a culture of security. Inferentially, the Sexting vignette might be suitable for a possible explanation. Although morality perception means were “lukewarm” (people rated it as acceptable or reproachable or neutral), engagement perceptions were very low. It may be that the sample (N=709), because of its particular demographic qualities and high levels of self-control, were less likely to engage in risky activities. In terms of age, this was a young adult sample with high levels of dispersion (M=28.36, Mode=23, SD= 10.02) and it comprised mostly university students and professionals. It may be that such a sample was well aware of the possible risks in sharing erotic pictures of themselves, but at the same time their answers may be based on what is socially expected from them (social desirability bias). The questionnaire vignettes are projective; therefore, they do not represent unquestionable evidence as to whether or not the participants engaged in the activities they were rating.

Finally, after the discussion on the existence (or lack thereof) of a culture of security and a false sense of security, the cyborg neutralisation item that has been named “the culture of security” is theorised by the present researcher as:

An explicit or implicit lack of knowledge of socio-cultural norms (including legal norms) regulating the use internet (and/or any information and communication technology device) that can facilitate the commission of cybercrime. Also, in opposition, a perceived sense of security on the internet that can facilitate the commission of cybercrime and/or reassure the offender after the commission of cybercrime.

### **6.3. Cybercrime and Gender**

The Sexting vignette sparked considerable debate in this thesis because of its particularities. The scenario in the questionnaire depicted the following situation:

Gena is a 16 year old young girl that thanks to a social network has befriended a 31 year old man called *Bad\_Wolf* and started a relationship of sexual undertones. One day *Bad\_Wolf* asks Gena to send some naked pictures of her, she agrees and does it.

Respondents were asked, in the survey, to place themselves in Gena’s position, rate the case morally, indicate whether or not they would engage such behavior and how would they justify their behaviour. It is important to repeat that they were asked about Gena and her sending naked pictures, not about *Bad\_Wolf’s* relationship with a minor girl. They were asked to rate a character who is female, a minor and is engaging in active sexual activities, acting overtly about her sexuality. According to the text, Gena was not coerced into sending the naked

pictures; she did it of her own volition. This was the only case that did not constitute any illegal wrong (criminal or otherwise) in Spanish legislation.

The Sexting vignette has a sequel or even a parallel in the Revenge Porn vignette, drafted in a different way:

Peter and Susan were going out. Susan used to send suggestive pictures of herself via e-mail accompanied by saucy messages. One day Peter discovers Susan is having an affair and he decides to take revenge on her by sending her pictures and messages to his friends via social networks and e-mail, as well as posting them on the internet.

In this case, participants were asked to rate Peter, who had disseminated naked pictures of his girlfriend on the internet out of scorn. Peter actions were rated as very morally reproachable ( $M=9.20$ ) and engagement was very low ( $M= 0.46$ ). In fact, this morality mean was the highest of any vignette. Yet it was Susan who sent Peter the erotic pictures, as Gena had done. It is possible that the Revenge Porn vignette acted to warn participants of the risks involved in sending sexually explicit pictures to someone, as it preceded the Sexting vignette. This knowledge may have affected their engagement responses in the sexting case?

When comparing the engagement and morality means by using T-Tests and gender as the grouping variable, all the mean differences were statistically significant, following the patterns that emerged during the analysis of the survey data (males showed higher engagement and females higher moral reproach in all vignettes). The exception was found in the sexting morality question (see Figure 13), where the difference between morality means were not

statistically significant in relation to gender, and are very similar between male and female respondents. Both males and females were morally neutral about female minor sending naked pictures of herself to an adult. It may be that they approached the cases from a perspective of absolute sexual freedom, a feminist liberation perspective or maybe even from a perspective of masculine hegemony (Juschka, 2009).

The present work has identified several issues that call for a discussion of gender. These issues comprise sexuality on the internet, sexting and pornography. This discussion has arisen not only from the Sexting vignette, the Revenge Porn vignette and the Cyberstalking vignette, but from the recurring references to pornography throughout the interviews .

### **6.3.1. Sexuality and pornography on the internet**

The idea of the cyborg is fundamental to this present thesis, as is the idea of *Apparatgeist*. In terms of sexuality, these notions become of the uttermost relevance. Haraway's discourse is essentially a feminist one (her seminal book cited in this research is called *Simians, Cyborg and Women: The Reinvention of Nature*) and has spawned a recognized trend of *cyberfeminisms*.

She argues that:

The cyborg is a creature in a post-gender world; it has no truck with bisexuality, pre-oedipal symbiosis, unalienated labour, or other seductions to organic wholeness through a final appropriation of all the powers of the parts into a higher unity. (Haraway, 1991, p. 150)

The cyborg, according to Haraway, transcends the idea of gender. At the core of the concept lies the idea of escaping what is human and what is technological in our nature, and becoming something more that is both and neither. Boler (2007) indicated how authors have recognized in the qualities of cyberspace “the potential for challenging notions of fixed and static identities, for fluidity of identity through gender play and an escape from binaries” (p. 149; see also Jewkes & Sharp, 2003, for a discourse on internet identity).

Online pornography represents in a way, sex with, and through, the cyborg construction. Cronin and Davenport (2001) analyse pornography from the theoretical standpoint of a social shaping of technologies - an approach not dissimilar to Katz and Aakhus' *Apparatgeist* (2002), which examines how social norms shape the use of technology and vice-versa. In Cronin and Davenport's discourse, pornography production and consumption are defined by the demands of electronic commerce and technology. “The world of cyber pornography is a compelling, impulse-driven market with, by some counts, more than 30 million unique visits being recorded daily” (Cronin & Davenport, 2001, p.43). They offer, perhaps, a much positive account of what they seem to understand as a budding business with, multiple personal and social advantages. For Cronin and Davenport, consumers can benefit from interactivity, comfort, control and relative anonymity, where the internet becomes a “sanitized” (p.43) environment far from disease and shame, a cyborg haven where bodily constraints hold no significance whatsoever. The cyborg metaphor can be taken to the extreme, with Cronin and Davenport referring to the use of wearables and immersive hardware that grant a quasi-real sexual experience with a real-life partner or a performer. However, cybersex (or cyborg sex) is not entirely safe from “disease”. C13 (The Police Porn Virus) is important here; with the perverse allegory regarding sexual infection found in NPEX2's discourse. NPEX2 described how, in C13, a computer virus was inserted into pornographic content, such that user's computer



became infected when they accessed that content: “What is something everyone visits, well, child pornography web-pages; sorry pornography, not child pornography just pornography” (NPEX2, C13<sup>xciii</sup>). As discussed in the law enforcement agents’ interview findings, NPEX2 praised the quality of the virus design, and its capacity to spread by using instruments of globalisation and social engineering. Helmreich (2000), coming from a cultural anthropological perspective, studied the biological rhetoric of computer virus infection, their figurative penetration and invasion of the “body”, and the health discourse attached to their prevention and treatment. Once the user enters the internet “it holds the threat of plunging the user into a disorderly and dangerous universe of encounters with strangers that are almost sexual in their character” (p. 477-478). This relates well to NPEX2’s account of the efficiency of the dissemination of the Police Porn Virus; a point reiterated by Helmreich: “the biological metaphor is often extended beyond comparisons with the infection of an individual, placing viruses within the larger context of an evolving population” (p. 475).

Returning to Cronin and Davenport’s positive analysis of online pornography, these authors also discuss the role of women in pornography, either as consumers or performers (2001, pp. 44-45). They indicate that the pornography business pays attention to the habits of women consuming porn, as well as the welfare of (female) performers. But they also address the existence of an ideological divide and debate in terms of pornography and feminism (2001, pp.44-45). This debate is important in this research when account is taken of the cybervictimisation of women and children. On the one hand, Tsatsou (2012) describes the two sides of the feminist discourse on cybersex “a women’s victimization perspective” or “a women’s liberation perspective” (p. 520). The victimisation perspective has been discussed in the present work already, with reference to grooming, harassment and child sexual abuse. Contributing to this discourse, Harrison (2006) contends that there was no difference between

pornography and child pornography, as they represent the same inequalities and overwhelming masculine hegemonies. She adds that the architecture of the internet, and the absence of limits on the content and depiction of violence or degrading behaviour “have contributed to an escalation in offending” (p. 371), and a “desensitizing” (p. 371) effect on young consumers of pornography and violence. Fisher and Barak (2001) warn about the use of “pornography” as an umbrella term when referring to concepts such as erotica, or even violent pornography. If these “categories” of pornography were adequately labelled they could offer relevant information on the effects of the consumption of pornography (p. 315). Most importantly, according to Fisher and Barak (2001), experience of internet sexuality will shape and affect the future sexual responses of individual to sexual stimuli. Internet pornography is then, according to Fisher and Barak having a psychological impact on the individual, yet at the very same time it affecting social structures or is affected by them.

Another debate on pornographic content and child pornography was raised by Reeves (2013), when analyzing “Second Life *ageplay*” (acting out as children in Second Life, for various purposes). Sexual ageplay is defined by Reeves (2013) as:

Not simply an image of virtual child sexual abuse (a sophisticated drawing of abuse), but it is the act of simulated virtual child sexual abuse: sexual ageplayers manipulate their avatars to interact and engage in sexual acts within the online world (p. 238)

It must be borne in mind that these child avatars are operated by consenting adults, during a fantasy in an online world. A market has arisen, though, for the trading of these images. Reeves (2013) considered different propositions relative to the link between sexual ageplay and child sex abuse - the creation of a paedophile community and the reinforcement of inappropriate feelings towards children. Reeves concludes that there is not enough evidence to support these concerns and recommends “in the interim, to prohibit sexual ageplay in the

registration, license and bail conditions for known sex offenders, and for those subject to sex offender orders” (p. 245).

From a masculinity point of view, Garlick (2010) provides a discourse on male hegemony and online pornography:

Of central importance is the illusion of technological control that the Internet offers over sexual experience via the enframing of nature—a calling to order in the name of securing hegemonic masculinity. The ability to access pornographic images of every variety on one’s computer screen in an instant seems to fulfill the desire to reveal sexuality in the form of a standing reserve that makes bodies and acts available to reinforce the existing gender order. (p. 610)

This hegemony is not only domination over women and the perpetuation of gender inequalities. It goes far beyond this, as it refers to control over nature, by the capacity of “enframing nature” - capturing it, cataloguing it, disembodiment the sexual act and the performers, and classifying it by thematic tags on the internet, and making them available or searchable. Bodies are thus “merely resources, calculated and catalogued in advance, the life sucked out of them, circulating as empty forms within a largely commodified digital economy” (Garlick, 2010, p. 612). Sex, individuals and nature are demoted to fungible goods to be exchanged and accessed following the diktat of capitalism.

### 6.3.2. Sexting, gender and cybervictimisation

A gendered approach is necessary in trying to understand how cybercrime affects children, females and males differently, and essentially why some of the practices were perceived differently or similarly by male and female respondents. The Sexting vignette became one of the cruxes of the survey findings.

Sexting is, from a cultural standpoint, a consequence of a media-dominated society. Curnutt (2012) describes the relationship between sexting, Twitter and the celebrity culture:

If the libidinal economy supporting the mainstream media's eroticization of teenage sexuality is in some way the byproduct of the mechanisms that regulate the media industry's depictions of sexuality (e.g., rating systems and ordinances prohibiting underage nudity), then the enjoyment found in these depictions corresponds with the manner in which they implicitly transgress, without explicitly violating, the law. (p.363)

Therefore, sexting becomes a borderline legal/illegal practice that cannot really be considered deviant in its generality. At the same time, boundaries between an intimate practice and a public practice (like the emergence of the *selfie* culture, for example) become blurry:

However, sexting does not necessarily have to be classified as an exclusively private or public activity. Instead, it can be thought of as a sometimes-private/sometimes-public practice that relies on a level of reflexivity for its participants to remediate themselves in accordance with the institutional discourses and conventions that govern the media

industry's production of sexual imagery for a heterosexual male audience. (Curnutt, 2012, pp. 360- 361)

According to studies carried out in the UK, "Indecent images of children (IIOC) continued to proliferate across the internet with no single means of storage or distribution achieving overall dominance in 2012" (CEOP, 2013b, p.8) and "120 of the victims depicted were female and 26 male" (CEOP, 2013b, p. 9) meaning "An overall increase in the number of female children in images. A 70% increase in female victims aged under ten and a 25% increase in female victims aged over ten" (CEOP, 2013b, p. 9). In regards to self-generated indecent imagery (SGII), it has been found that "the majority of this imagery as having been freely produced by young adolescents in the course of developmentally appropriate behaviour not involving coercive or exploitative conduct by an adult" (CEOP, 2013b, p. 12) - as depicted in the Sexting vignette from the online questionnaire. In terms of the gender, the research indicates that for all forms of SGII (still and moving) 18% of individuals featuring in these images are male and 82% female these cases, data indicates the following percentages divided in still and moving SGII: males 18%, whereas females 82 %. In respect of moving SGII 55% of featured individuals are male and 37% female. Females, therefore, are much more prone to share still pictures, whereas men are more keen on moving imagery (videos)(CEOP, 2013b, p. 12). CEOP warns that "In stark contrast, moving images also showed a greater tendency towards more sexualised content than still imagery, with 10% depicting penetrative sexual activity" (CEOP, 2013b, p.12).

In Spain, the case is different. *Instituto Nacional de Telecomunicaciones* (National Telecommunication Institute, INTECO<sup>24</sup>) and the mobile company, Orange, found, in relation to sexting that, "in Spain, 4% of minors in between 10 and 16 years old admits to have taken

---

<sup>24</sup> Now called *Instituto Nacional de Ciberseguridad* (National Cybersecurity Institute, INCIBE)

pictures of themselves or videos in a sexy pose (not necessarily naked or erotic) using a mobile phone” (INTECO & Orange, 2010, p.87<sup>xciv</sup>). In contrast, 8.1% admitted receiving sexually provocative pictures from others (INTECO & Orange, 2010, p. 87). There is no data on gender relative to these practices. Strassberg, McKinnon, Sustaíta, and Rullo (2013) undertook an exploratory study of sexting by high schools students and after a gender comparison they discovered that more male students than females reported having received a sext, yet “the groups did not differ in the percentage of students reporting having sent a sext of themselves” (p.18). There is very limited data on sexting in Spain (which is surprising as it does seem to be a quite common practice among minors) including the gender of those involved in it. However, it does appear a practice that involves both sexes. Rollins (2015), studied the outcomes of several sexting legal cases in the USA and found profound differences in terms of gender in the rulings. In his study, three rulings are compared:: one case involved teenage girls keeping pictures of themselves scantily clad (but no naked or pornographic content). Another case involved a male high school student that tricked other male students into sending naked pictures to him. (He facilitated this ruse by pretending to be a flirtatious girl on the internet. He ended up manipulating the other male students into having sex with him and taking photographs of the acts.) The final case discussed by Rollins (2015) concerned a hockey coach who started a relationship with a 16 year old girl and took pictures of both of them having sex, and then sent these pictures to the girl. After a discussion on gender, sexuality and childhood, Rollins (2015) reached the following conclusions:

Child sexual abuse is perceived as more damaging to boys because it threatens to undermine their gender training as sexual agents. Girls, meanwhile, are expected to assume their properly gendered role as sexual objects; sexual abuse of girls is part of the norm. (p. 66)

And,

Sexual agency and object status remain gendered but the underlying power dynamic is no longer so closely aligned with sexual orientation; the primary axis of tension is now becoming age. (p. 67)

Each of the reflections above may help explain why the sexting case contained within the online questionnaire, in the present thesis, obtained such morally discrepant results, featuring as it did a 16 year-old girl exerting sexual agency. For some people, she might be acting “saucy” and would have to face the consequences of her actions; whilst for some others she was just doing what any youngster would do, regardless of gender. For some other people, the “moral key” might lie in the fact that she is 16 (not that she is a girl) and she is sharing pictures with an older male (*Bad\_Wolf*), therefore shifting the tension from gender to age. On the other hand, this tension between gender and age could explain why vignettes, such as those involving Revenge Porn and Cyberstalking, obtained such high moral reprobation. In both of them, it could be assumed that the characters are of the same age, involved in, initially, socially licit dynamics. In the Revenge Porn vignette, the characters were going out together, whereas in the Cyberstalking case they were workmates. In both cases, the male protagonists were acting predatorily against women (even though in the Revenge Porn vignette, the female protagonist also exerted sexual agency by sending erotic pictures to her boyfriend).

It should be noted that there were some leading words in the instruments that might need to be modified and/or corrected for further research. First, the idea of using the nickname *Bad\_Wolf* in the sexting case was supposed to be ironical, yet it could have tampered with the respondent’s perception of the situation. In addition, the gender of the individual sending the picture was said to be female. This may have had an impact on the way in which participants responded to this vignette. After much thought from part of the researcher, as it could

generate a gender bias. It may, in fact, have been better if all the vignettes had been gender-neutral in order to avoid such problems or at least more varied in terms of gender. Similarly, the present researcher now feels that it was not necessary to add a coda to the cyberstalking scenario – “Deborah feels very uncomfortable and scared about this”, and again this may have had the effect of leading participants to give particular answers.

#### **6.4. Brief Summary of Current Cybercrime Prevention and Cybercrime Policy**

The present thesis is not primarily concerned with crime prevention. However, it is felt to appropriate briefly examine current instruments for the prevention of cybercrime both in Spain and the UK, given that implications regarding this have emerged from the present research. Welsh and Farrington (2012) have described the different paradigms in crime prevention, albeit from a US perspective. Developmental crime prevention is “informed generally by motivational or human development and life-course theories on human behaviour” (Welsh & Farrington, 2012, p. 8). This approach draws upon empirical studies in order to design prevention programmes, focusing essentially on youngsters. “Community crime prevention” (pp. 9-11) is centred on how the social climate can affect communities and their stakeholders, and how manipulating those conditions can help prevent crime. Situational crime prevention differs from the other paradigms because of its “special focus on the setting or place in which criminal acts take place” (p. 11). In the case of situational crime prevention, the emphasis is placed not on the person or the social structure, but on opportunities for committing crimes and the physical deterrence of crime (for example, building fences and installing CCTV).



In relation to cybercrime prevention, Wall (2007) talks about preventing crime by using technology (pp. 187-192). He summarises the technological approaches as “designing crime out of systems or designing crime control into them” (p. 187). These are, essentially, situational crime prevention techniques. Wall also refers to “digital realism” when explaining cybercrime control by using the law:

law does have the capacity to shape not only the environment that influences the formation of the code which forms the architecture of cyberspace, but also the social norms which internet users take with them online and the incentives and disincentives created by the market which shape the behaviour within (p. 192)

Therefore, the prevention of cybercrime can be understood from two distinct approaches: the opportunity one and the legal-behavioural one.

In respect of preventing cybercrime, Buono (2014) suggests using strategic intelligence analysis to gain “a clearer picture of the gangs involved in cybercrime modi operandi and cybercriminals’ motivations” (p. 3), international cooperation, and awareness raising and the education of users. An example of education of users will be represented by law enforcement’s use of social media in Spain. An example of international cooperation in Spain is represented by the integration of Spanish Policing in the European Cybercrime Centre (CNP, 2013a, 2013b). The use of intelligence analysis was alluded to by NPEX1, when he pointed out that he belonged to an intelligence gathering unit (named “open sources”). He also described the use of intelligence gathering techniques and software for the investigation of C10 and C11: “then you go and input the data, complaint by complaint, and it makes these schemes, and it

gives you the relationships” (NPEX1, C11<sup>xv</sup>). He revealed that these tools were a great aid in his investigation and in the presentation of findings to judges.

In relation to the legal-behavioural approach mentioned by Wall (2007), several changes in the current criminal code have been introduced to counteract certain cybercrimes (see Chapter 2: Literature Review). In this way the Spanish Criminal Code acknowledges the ubiquity of cybercrime and seems to recognise the existence of new criminal activities arising from the development of new technologies or simply the adaptation of older crimes into cyborg constructs. The definition and tackling of cybercrime has occurred gradually in Spain, yet the instruments used are still too embryonic to test their efficiency in preventing cybercrime.

In the UK (see also Chapter 2: Literature Review), for example, the Coroners and Justice Act 2009 includes the concepts of “pseudo-photograph”, incorporates electronic data in the formats of “indecent photograph” and makes reference to “imaginary children”. In addition, the Sexual Offences Act 2003 criminalises child grooming, and the recent Criminal Justice and Courts Act 2015 prohibits the disclosing of private sexual images or film with the intention of causing distress and the possession of pornographic images or rape or assault. The UK has, therefore, elevated Revenge Porn to crime status.

In terms of policing, Wall (2007) talks about different stakeholders policing the internet, including internet users , moderators of online communities , ISP’s , corporate security , non-governmental bodies, non-police organizations, governmental non-police organizations and public police groups . In Spain, as has already been pointed out in this thesis, the Guardia Civil and the Policía Nacional have different cybercrime units (UIT for Policía Nacional and GDT for

Guardia Civil). There also exists the INCIBE (formerly INTECO) is the Spanish National Institute for Cybersecurity, governed by the Ministry of Industry, Energy and Tourism. These are examples of public police groups and governmental non-police organizations in Spain.

The police and the Guardia Civil are both trying to encourage community-based policing by using social networks). One of the most visible manifestations of the online community is the creation of the @policia Twitter account (already mentioned in the LEA interview findings). (@guardiacivil is following their steps closely, and Instagram and YouTube accounts, and Facebook pages have been created lately by these law enforcement bodies). In trying to reach the general public, they have amassed a huge following and almost achieved a cult internet status. The prevention emphasis is placed on the eventual victim and on situational crime prevention (Clarke, 1999; Cornish & Clarke, 1986, 1987; Miró Llinares, 2011; Newman & Clarke, 2003; Yar, 2005). The National Spanish Police also organize courses with schools and parents in order to teach students and families about problems arising from internet misuse, and they also seek to minimise the already mentioned “generational digital divide”.

The National Cyber Crime Unit (under the National Crime Agency) in the UK “leads the UK’s response to cyber crime, supports partners with specialist capabilities and coordinates the national response to the most serious of cyber crime threats” (NCA, 2015). The National Cybercrime Unit works as a multi-partner agency that carries out intelligence gathering and advisory duties, and pursues cybercrime at a national and international level. The Metropolitan Police Cyber Crime Unit works in partnership with the National Cyber Crime Unit and is charged with investigating several types of cybercrime. Finally, CEOP is also part of the National Crime Agency, and investigates the abuse and exploitation of children online. At the

same it tries to educate and raise awareness among children, parents and educators with several sites and social networks accounts<sup>25</sup>. CEOP, in its 2013-2014 Centre Plan and 2012-2013 Annual Review identified four strategic themes: setting priorities and coordinating the delivery of a response; supporting operational delivery and the development of new capabilities; building and maintaining specialist and mutually beneficial relationships; and providing and supporting an expert workforce (CEOP, 2013a). Education and awareness rising in children is one of its fundamental priorities (CEOP, 2013a).

The new adjusted model, with its circuit of cybercrime, could work as a tool for cybercrime prevention. Programmes could focus on any of the steps of the circuit, maybe on all of them. Instead of working with a victim-based criminology, it may be time to focus on the different stages that lead cybercriminals to the commission of crimes. This may be especially relevant in light of the fact that cybercriminals are not ontologically criminal, written and programmed from crime, but are individuals with a level of self-control and propensity that, at a given time, enter into contact with the internet. At the same time, emphasis should also be put on the macro-structures that transmit frustrating messages (like the capitalistic drive, for example) and there should be a rethinking of the ways in which individuals interact with the internet.

## **6.5. Limitations**

The first essential limitation found in relation to the online survey concerns the sample, as it is comprised mostly of university students. This demographic overrepresentation might have

---

<sup>25</sup> For example, the twitter account @ThinkuknowUK

resulted in certain perceptions of morality or self-control measures. That overrepresentation might have occurred because of the absence of a randomization procedure. The characteristics of the sample could be seen as an inherent limitation of the study, as an educational and/class bias could be present because many of the respondents are educated and affluent attending a private university. In addition to this, there are no minors in the sample and no self-reported criminals either.

Having access to individuals who had committed cybercrimes should have provided more reliable data on the use of neutralisations and crime propensity. One could argue that some of the survey respondents might have committed some of the behaviours depicted in the vignettes. More specifically, those rated as morally acceptable and/or those they as acceptable to engage in, according to Wikström et al. (2013) that tends to be the case. The online survey sample, also, tended to overrepresent law enforcement agents, lawyers and university students. Another limitation is related to the instrument, especially the presentation of the vignettes, as some of them might be gendered-biased (the Sexting vignette and the Cyberstalking vignette, for example).

The questionnaire survey sample was not entirely representative of the general population of internet users. In regards to the “captive” audience (those surveyed in the classroom), the demographic leant towards affluent young students studying at a private institution in Spain. There also existed a slight imbalance within the sample, in terms of gender (60% female, and 40% male). When the questionnaire was disseminated on the internet, it drew its respondents primarily from the researcher’s contacts, creating an educated sample, comprised mostly of university students, lecturers, lawyers and police officers. Minors (people aged less than 18 years) were not represented (as far as author knew). The less than 18 year old age group

would have been very interesting in terms of cybercrime, attitudes and neutralisation, as it would have included the so-called “digital natives” or “millennials”, whose contact with technology and exposure to the internet is more extensive than any other group. Also, high-levels of self-control might be expected from a sample that is, theoretically, generally comprised of “non-criminal” individuals and collectives with strict views on morality (for example, police officers).

In relation to the law enforcement agents’ interviews - even though the number of interviewees might be considered small - the catalogue of cases is varied and all of the interviewees have considerable experience in the investigation of cybercrimes. One of the major issues that has been discussed thorough this work is the possible existence of an ideology and a police discourse.

One major limitation of this study is that it did not explore the subjective reality of cybercriminals. As indicated in previous paragraphs, and from a qualitative point of view, it drew conclusions from “proxies” (law enforcement agents) and their construction of criminal identity. This construction, as rigorous as it may have been, may also have been contaminated by cultural perceptions (there are no studies of police culture in Spain). First-hand narratives of cybercriminal identities could have explained the reasons why neutralisation techniques were used, or why and how this propensity towards cybercrime was forged. Moreover, interviews with cybercriminals themselves would have helped understand the psycho-social rapports established with the computer world and how these affect the development of criminal/non-criminal narratives. Having said this, several practical and ethical issues would likely have emerged from trying to use such a sample, including gaining access to a very elusive sample and the practice of online ethnography (Hooley et al., 2012). All of these issues had to be

taken into account by the researcher when he designed the methodology, faced as he was with time, budget and access constraints.

Finally, in relation to the adjustment of the theoretical framework as the “circuit of cybercrime” the following issues arose: the first issue (generated by the mixed methods design of the study) is that “Cyborg Neutralisation Items” (CNIs), have not yet been tested after their emergence. The second limitation is found in the discussion of whether some of the data that emerged after the case study are either neutralisation techniques or cognitive distortions (essentially in all the cases that related to online child sex abuse). This is the reason why, in the final adjustment of the “circuit of cybercrime”, cognitive distortions (cognitions) have been added to the model as they would fulfill the same role neutralisation techniques do in the theory.

## **Chapter 7: Conclusions**

### **7.1. Summary of Findings**

The present thesis explored whether the SAT model required adaption in order to explain cybercrime. The adapted model (SAT-RI) aimed to explain the reasons why people commit cybercrimes. It aimed to do this by taking into account the basic elements of SAT: crime as a process of deliberation occurring when any given individual's crime propensity interacts with an environment that is conducive to crime. SAT sees the moral norms of the setting and the individual as the core elements in crime causation, as well as the mediating role of self-control. In addition, SAT-RI takes into consideration any given individual's cybercrime propensity when interacting with the internet (as a setting) and also the effective application of a neutralisation technique. It, too, considers the role self-control plays.

The mixed methods study seemed to support the need for a development of the SAT model into the SAT-RI model, although data pointed towards a different relationship between variables than the one originally theorised. The analysis of data (online survey and law enforcement agents' interview data) resulted in the creation of what has been named "the circuit of cybercrime": a sequential explanation of the commission of cybercrimes based on the "flow" of self-control, cybercrime propensity (measured as the perception of morality of cybercrime and the possibility of engaging in cybercrime) and the use of specific neutralisation techniques to facilitate the commission of that kind of crime (or the inability to neutralise a crime). Unanticipated factors were added to the "circuit of cybercrime". These elements are referred to as "Cyborg Neutralisation Items" (CNIs). These items are very specific kinds of neutralisation, which stem from broader social/structural issues that become relevant when



considering the organic and transformative relationship forged between society, machines and the individual. These CNIs, however, are in need of further testing. It is important to note that SAT-RI could help explain the reasons behind the commission of any type of cybercrime, but solely cybercrimes. In addition, the concept of cybercrime presented in this essay transcends strict legal definitions in order to consider any form of cyberdeviance (for example, trolling). From a different point of view, what the theory aimed to address are the transformations operated by the advent of digital technology within society and the changes it has produced anthropologically (for example, the change in customs, relationships and sexual behaviour), and how the onslaught of that “becoming” has produced several dysfunctional responses (cybercrime, for examples).

## **7.2. Further and Future Research**

Future research should test the new adjusted model, including the already mentioned “Cyborg Neutralisation Items” (CNI) either from a quantitative, qualitative or mixed methods approach. The CNIs emerged “ex post” interview analysis and were added to the initial SAT-RI model. It would be necessary to explore -based on definitions of CNIs suggested by the present researcher- their role in justifying cybercrime and their role in affecting the morality and engagement variables.

Also, future research should also try to obtain a larger and more diverse sample in any online survey that is carried out - one which includes minors and respondents from the UK, to enable comparisons between generations and countries. A study, similar to the present work, but on a national level, should be conducted in the future, profiting from the viral nature of

social networks, but also making use of face to face administered questionnaires (as it was done in different classrooms). This study should utilise a multi-clustered, probabilistic sample, drawing upon different schools and universities across Spain. It would be necessary to survey a sample that is more representative of the general population. Future research, if using vignettes to measure attitudes towards cybercrime should aim to use questions that are gender neutral and are devoid of any leading elements.

Also, police officers from other countries should be interviewed in order to gain a better understanding of the cybercrime phenomenon, and to compare ideologies and law enforcement discourses to determine their differential impact upon police perceptions of offender motivation. A study on Spanish police culture (be it in relation to the investigation of cybercrime or police culture in general) is needed in order to shed light on how the notions of crime and the criminal are constructed by Spanish police officers.

From a different perspective, online ethnography (Hooley et al., 2012) studies seem necessary. Online message boards, blogs and social networks generate immense amounts of data and serve to guide trends and opinions (Connor, Coombes, & Morgan, 2015; Servera, 2014a). Holley et al. (2012) advocate the use of online ethnography in order to capture the richness of human experience in the online world. Hooley et al. also indicate that the internet offers more and more opportunities for research given “the vast expansion of naturally occurring online data” (p. 89). By using this method, more will be learnt about offender motivation; behaviors and the way offender construct their identities online. Online ethnography would also be a very effective tool in order to understand budding social movements (for example hacktivists) or online subcultures. Moreover, online ethnography could also be used in order to study, understand and contextualize pornography and paraphilia in the online world. By doing this,

more will be learnt about offender motivation; behaviors and the way offender construct their identities online.

Finally, the most valuable research that could be conducted is that with cybercriminals. Interviews should be conducted with all types of cybercriminal including, for example, fraudsters, virus designers, online child sex abusers and child pornography users. A qualitative approach is recommended in order to gain a deeper understanding of their motivations and perceptions, and to determine how different types of cybercriminals assign meaning to their personal narratives. Research on cybercriminals could be complemented with qualitative document analysis (Bryman, 2012) using case rulings about cybercrime as source of data, as well as newspaper and magazine articles. Data on the media portrayal of cybercriminals and cybercrime would be very valuable in order to understand cybercrime as a cultural narrative (Wall, 2008a, 2008b).

### **7.3. Implications**

#### **7.3.1. Prevention programmes based on SAT-RI**

The “circuit of cybercrime” represents the moral deliberation process as follows (Figure 23): self-control can affect crime propensity and the use of non-neutralisations, at the same time the use of non-neutralisations affect crime propensity.

On the other hand, the use of efficient neutralisation techniques can affect crime propensity. Also, it is theorised, cognitive distortions and “Cyborg Neutralisation Items” (CNIs) have

analogous effects to neutralisation techniques, being able to also affect crime propensity (this has not been tested as it has been theorised *ex post* data analysis).

Prevention programmes should aim to truncate the flow of the “circuitry”. One of the key elements to be tackled should be the use of neutralisation techniques. Effective neutralisation techniques should be identified by future research, which policy-makers could then act upon. An emphasis should be placed upon personal responsibility and personal agency, for example, trying to transmit to either the general public or a specific cohort that cyberbullying is not a game between children but can be a crime with serious consequences. In terms of illegal downloading, work might need to be undertaken by policy-makers (and even entertainment companies) in disseminating and reinforcing a solid understanding of the law in relation to intellectual property or redesign the “streaming market”.

### **7.3.2. A new paradigm for approaching cybercrime: "cyborg criminology"**

At the end of the second chapter of this thesis, six postulates were presented as foundation of the SAT-RI:

- 1) It is a theory that serves as an explanation of cybercrimes only (albeit all types of cybercrime).
- 2) It operates under a broader definition of cybercrime presented in Chapter 2 that also includes deviant cyber-behaviour (for example, trolling).
- 3) It considers that the mere exposure to the internet is criminogenic in itself, therefore exposure will be treated as constant (in the propensity x exposure x neutralisation model). On the other hand, self-control, cybercrime propensity and the use of neutralisation techniques are going to be measured.

- 4) It does not pay attention to the device the internet is accessed from (computers, wearables, and smart phones, for example).
- 5) It considers the whole of the internet as the setting and does not make any distinctions as to whether the user is accessing the surface internet or the darknet (or deep web).
- 6) It tries to consider the impact of the advent of digital technologies on human nature, behaviour and identity.

Several issues relating to some of the postulates (especially the sixth postulate) arose during data analysis and even more so in the course of preparing Chapter 6 – the integration of the survey and interview data. These issues were well exemplified in the discussions about pornography, narcissism in social networks and compulsive consumerism (see Chapter 6). One of the best examples, perhaps, of the effects of digital technology lies in the “death by selfies” incidents (ABC, 2015; El País, 2015; Golby, 2015; Ruiz Marull, 2015): people that end up dying in their search for a perfect selfie, for example falling from a precipice or shooting themselves accidentally. The death by selfie serves as a tragic example of the ultimate ontological sacrifice - dying because of the “becoming” cyborg. The sacrifice is represented by the fact that the necessity to post a picture in social networks outweighs personal security. In parallel, this sort of “cult to oneself” creates a new breed of excess celebrity culture, like the one represented by Dan Bilzerian (Millard, 2015), who has amassed millions of followers on Instagram and Twitter by posting about his excessive lifestyle; one dominated by guns, planes, scantily clad women, and swimming pools. Another example of this phenomenon is the “Youtuber” in which “average regular people” becoming celebrities and cultural influencers. The normalisation of criminal and/or deviant activities, such as sexting, amongst young people, or the construction

of the illegal downloading of movies as a daily “everyday habit”, also pointed towards changes brought upon mankind by the proliferation of digital technologies. Moreover wearables, the Internet of Things (IoT), Augmented Reality and the Cloud create a multi-layered network of humans, objects and data, all of which incorporate crime prevention capabilities or, contrarily, criminogenic properties (see Europol, 2015; Servera, 2014, 2015).

All in all, a new criminological approach to cybercrime, which tackles all of the issues discussed in the previous paragraphs, could offer a fresh view on the dysfunctional aspects of human behaviours stemming from the human/machine interface. Studies on cybercrime have focused more on the manifestations of cybercrime, its evolution, its regulation and prevention, and its repercussions (essentially economic), rather than on the human cost of the networked society and its psycho-social impact. By contrast, other human sciences have tackled issues such as addiction, deviance, sexuality, identity and eventually transcendence (to the trans-human, then the post-human) to great avail (Haraway, 1991; Jewkes & Sharp, 2003; Vicini & Brazal, 2015; Wells, 2014). Criminology, understood as a multidisciplinary science (Herrero Herrero, 2007; Garrido et al., 2013), could benefit from the use of more psychological, social and/or anthropological approaches to cybercrime.

The initial postulates of cyborg criminology would be:

- 1) A criminology that considers the impact of digital technologies upon all facets of human behavior, and studies the emotional rapport forged between mankind and digital technology (essentially the internet).
- 2) A criminology that considers the forms of crime created by the proliferation of digital technology and by the mankind/machine interface, but also deviant behaviour and/or dysfunctional attitudes, such as, among others, addiction, obsession, inequality (including gender inequalities), sexual deviation, pathology, suicide.
- 3) A criminology that also incorporates an anthropological, philosophical, social, psychological, sexual, critical and cultural discourse on the relationship with machines.
- 4) A criminology that aims to develop and test criminological theories for the explanation of cybercrime under the previous postulates.

Such criminology might offer a very different perspective on cybercrime, especially if combined with other disciplines. In fact, the cyborg discourse as indicated by Haraway (1991) is essentially postmodern and eclectic: “cyborg imagery can suggest a way out of the maze of dualisms in which we have explained our bodies and our tools to ourselves. This is a dream not of a common language, but of a powerful infidel heteroglossia” (p. 181) Haraway adds

The machine is not an it to be animated, worshipped, and dominated. The machine is us, our processes, an aspect of our embodiment. We can be responsible for machines; they do not dominate or threaten us. We are responsible for boundaries; we are they. (Haraway, 1991, p. 180)

A cyborg criminology would, essentially, address broader issues than those generally discussed by cybercriminology and would be in tune with current cultural and technological development.



## References

- ABC. (2015, September 22). Mueren más personas por selfies que por ataques de tiburón [More people die because of selfies than because of shark attacks] . *Abc*. Retrieved from <http://www.abc.es/recreo/20150922/abci-muertes-serfies-ataques-tiburon-201509221233.html>
- Adeniran, A. (2011). Café culture and heresy of yahooboyism in nigeria. *Cyber criminology: Exploring internet crimes and criminal behavior* (pp. 3-12) CRC Press. doi:doi:10.1201/b10718-3
- Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, 30(1), 47-87.
- Agnew, R., Brezina, T., Wright, J. P., & Cullen, F. T. (2002). Strain, personality traits, and delinquency: Extending general strain theory. *Criminology*, 40(1), 43.
- Anderson, T. (2008, September 25). Is it all clear skies ahead for cloud computing? *The Guardian*. Retrieved from <http://www.theguardian.com/technology/2008/sep/25/computing.internet>
- Baudrillard, J. (1988). *Selected writings*. Cambridge: Polity
- Bauman, Z. (2000). *Liquid modernity* (1st ed.). Oxford: Polity.
- Benedikt, M. (2000). Cyberspace: First steps. In D. Bell, & B. Kennedy (Eds.), *The cybercultures reader* (pp. 29-45). London: Routledge.
- Boer, D. P., Merdian, H. L., Wilson, N., Thakker, J., & Curtis, C. (2014). The endorsement of cognitive distortions: Comparing child pornography offenders and contact sex offenders. *Psychology, Crime & Law*, 20(10), 971-993. doi:10.1080/1068316X.2014.902454
- Boler, M. (2007). Hypes, hopes and actualities: New digital cartesianism and bodies in cyberspace. *New Media & Society*, 9(1), 139-168. doi:10.1177/1461444807067586
- Brenner, S. W. (2007). "At light speed": Attribution and response to Cybercrime/Terrorism/Warfare. *The Journal of Criminal Law and Criminology* (1973-), 97(2), 379-475.
- Brenner, S. W. (2010). *Cybercrime :Criminal threats from cyberspace*. Santa Barbara, Calif.: Praeger.
- Briggs, D. (2013a). Capitalismo extremo, ideology and ibiza: A new perspective on youth deviance and risk on holiday. *Papers from the British Criminology Conference*, (13), 33-50.
- Briggs, D. (2013b). *Deviance and risk on holiday: An ethnography of british tourists in ibiza*. Hampshire: Palgrave Macmillan.
- Bryman, A. (2012). *Social research methods* (4th ed.). Oxford: Oxford University Press.

- Buono, L. (2014). Fighting cybercrime through prevention, outreach and awareness raising. *ERA Forum*, 15(1), 1-8. doi:10.1007/s12027-014-0333-4
- Burn, M. F., & Brown, S. (2006). A review of the cognitive distortions in child sex offenders: An examination of the motivations and mechanisms that underlie the justification for abuse. *Aggression and Violent Behavior*, 11(3), 225-236. doi:10.1016/j.avb.2005.08.002
- Carou, M., Romero, E., & Luengo, M. Á. (2013). Patrones de consumo y variables de personalidad en drogodependientes a tratamiento [Patterns of use and personality variables in drug addicts under treatment]. *Revista Española De Drogodependencias*, (3), 217-232.
- Castells, M. (2010). *The rise of the network society* (2nd with a new preface. ed.). Oxford: Blackwell.
- CEOP. (2012). *Threat assessment of child sexual exploitation and abuse 2012*. London: Child Exploitation and Online Protection Centre. Retrieved from [https://www.ceop.police.uk/Documents/ceopdocs/CEOPThreatA\\_2012\\_190612\\_web.pdf](https://www.ceop.police.uk/Documents/ceopdocs/CEOPThreatA_2012_190612_web.pdf)
- CEOP. (2013a). *Annual review 2012-2013 & centre plan 2013-2014*. London: Child Exploitation and Online Protection Centre. Retrieved from <https://www.ceop.police.uk/Documents/ceopdocs/AnnualReviewCentrePlan2013.pdf>
- CEOP. (2013b). *Threat assessment of child sexual exploitation and abuse 2013*. London: Child Exploitation and Online Protection Centre. Retrieved from [https://www.ceop.police.uk/Documents/ceopdocs/CEOP\\_TACSEA2013\\_240613%20FINAL.pdf](https://www.ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf)
- CEOP. (2015). Thinkuknow. Retrieved from <http://www.thinkuknow.co.uk/>
- Christensen, T. (2010). Presumed guilty: Constructing deviance and deviants through techniques of neutralization. *Deviant Behavior*, 31(6), 552-577. doi:10.1080/01639620903004929
- Clarke, R. V. G. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods*. (No. 112). London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.
- Clough, J. (2010). *Principles of cybercrime*. Cambridge, UK: Cambridge University Press.
- Clynes, M. E., & Kline, N. S. (1995). Cyborgs and space. *The Cyborg Handbook*, , 29-34.
- CNP. (2013a, May 16). Ignacio Cosidó destaca la lucha contra el cibercrimin como una de las prioridades estratégicas de la policía nacional [Ignacio Cosidó highlights the importance of the fight against cybercrime as one of the strategic priorities of the national police]. Retrieved from [http://www.policia.es/prensa/20130516\\_2.html](http://www.policia.es/prensa/20130516_2.html)
- CNP. (2013b, January 15). El plan estratégico de la policía nacional supone la transformación del cuerpo en una policía 3.0 [The strategic plan of the national police supposes the transformation of the corps in a 3.0 police]. Retrieved from [http://www.policia.es/prensa/20130115\\_2.html](http://www.policia.es/prensa/20130115_2.html)

Computer misuse act 1990, c. 18 (1990).

Connor, G., Coombes, L., & Morgan, M. (2015). iAnorexic: Haraway's cyborg metaphor as ethical methodology. *Qualitative Research in Psychology*, 12(3), 233-245. doi:10.1080/14780887.2015.1008901

Convention on cybercrime, (2001).

Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending*. New York: Springer-Verlag.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, 25(4), 933-947.

Coroners and justice act 2009, c.25 (2009).

Council of Europe convention on the protection of children against sexual exploitation and sexual abuse, (2007).

Creswell, J. W. (2011). Controversies in mixed methods research. In N. K. Denzin, & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research* (4th ed., pp. 269-283). Thousand Oaks: Sage.

Creswell, J. W. (2015). *A concise introduction to mixed methods research*. London: Sage.

Criminal justice and courts act 2015, c. 2 (2015).

Cronin, E., & Davenport, B. (2001). E-rogenous zones: Positioning pornography in the digital economy. *The Information Society*, 17(1), 33-48. doi:10.1080/019722401750067414

Curnutt, H. (2012). Flashing your phone: Sexting and the remediation of teen sexuality. *Communication Quarterly*, 60(3), 353-369. doi:10.1080/01463373.2012.688728

Delio, M. (2002, July 17). Meet the nigerian E-mail grifters. *Wired.Com*. Retrieved from <http://archive.wired.com/culture/lifestyle/news/2002/07/53818?currentPage=all>

Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). *Social media update 2014*. Pew Research Center. Retrieved from <http://www.pewinternet.org/2015/01/09/social-media-update-2014/>

Durkheim, E. (2013). In Lukes S. (Ed.), *The division of labour in society* [De la division du travail social] (W. D. Halls Trans.). (2nd ed.) [Amazon Kindle Version]. Basingstoke: Palgrave Macmillan. Retrieved from [www.amazon.es](http://www.amazon.es)

El País. (2015, July 9). Cómo evitar la 'muerte por selfie': La guía del gobierno ruso [How to avoid death by selfie': The Russian government's guide]. *El País*. Retrieved from [http://elpais.com/elpais/2015/07/09/tentaciones/1436456180\\_571915.html](http://elpais.com/elpais/2015/07/09/tentaciones/1436456180_571915.html)

- Empresa Municipal de Transportes. (2015). El portal de la movilidad 2.0 de la empresa municipal de transportes de Madrid [The 2.0 mobility portal of the municipal transport company in Madrid]. Retrieved from <http://www.emtmadrid.es/movilidad20/aplicaciones.html>
- Esin, C., Fathi, M., & Squire, C. (2014). Narrative analysis: The constructionist approach. In U. Flick. (Ed.), *The sage handbook of qualitative data analysis* (pp. 203-216). London: Sage.
- Directive 2011/92/EU of the European parliament and of the council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing council framework decision 2004/68/JHA , (2011).
- Europol. (2015). *The internet organised Crime Threat assessment (IOCTA) 2015*. The Hague: Europol. doi:10.2813/03524. Retrieved from <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015>
- Field, A. P. (2009). *Discovering statistics using SPSS: And sex and drugs and rock 'n' roll* (3rd ed.). Los Angeles, [Calif.]; London: SAGE.
- Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research*, 20(2), 303-315. doi:10.1086/209351
- Fisher, W., & Barak, A. (2001). Internet pornography: A social psychological perspective on internet sexuality. *Journal of Sex Research*, 38(4), 312-323. doi:10.1080/00224490109552102
- Fitbit. (2015). Fitbit official site for activity trackers & more. Retrieved from <https://www.fitbit.com/uk>
- Fox, J., & Rooney, M. C. (2015). The dark triad and trait self-objectification as predictors of men's use and self-presentation behaviors on social networking sites. *Personality and Individual Differences*, 76, 161-165. doi:10.1016/j.paid.2014.12.017
- Gannon, T. A., & Alleyne, E. K. A. (2013). Female sexual abusers' cognition: A systematic review. *Trauma, Violence, & Abuse*, 14(1), 67-79. doi:10.1177/1524838012462245
- Garland, D. (2000). The culture of high crime societies: Some preconditions of recent 'law and order' policies. *The British Journal of Criminology [H.W.Wilson - SSA]*, 40(3), 347.
- Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Oxford: Oxford University Press.
- Garlick, S. (2010). Taking control of sex?: Hegemonic masculinity, technology, and internet pornography. *Men and Masculinities*, 12(5), 597-614. doi:10.1177/1097184X09341360
- Garrido Genovés, V., Stangeland, P., Redondo, S., & Beristain, A. (2013). *Principios de criminología* (4a ed.). Valencia: Tirant lo Blanch.
- Gavin, H. (2014). *Criminological and forensic psychology*. London: SAGE.

- Goode, E. (2006). Is the deviance concept still relevant to sociology? *Sociological Spectrum*, 26(6), 547-558. doi:10.1080/02732170600948865
- GDT. (2013, November 16). Cryptolocker... cuenta atrás para destruir tus datos. [Cryptolocker... countdown to destroying your data]. Retrieved from [https://www.gdt.guardiacivil.es/webgdt/popup\\_alerta.php?id=218](https://www.gdt.guardiacivil.es/webgdt/popup_alerta.php?id=218)
- GDT. (2014, May 15). El virus “de la policía”... ¡ataca de nuevo! [The “police virus”... attacks again!]. Retrieved from [https://www.gdt.guardiacivil.es/webgdt/popup\\_alerta.php?id=220](https://www.gdt.guardiacivil.es/webgdt/popup_alerta.php?id=220)
- GDT. (2015, July 15). Estafas en alquileres vacacionales [Holiday apartment rent scam]. Retrieved from [https://www.gdt.guardiacivil.es/webgdt/popup\\_alerta.php?id=223](https://www.gdt.guardiacivil.es/webgdt/popup_alerta.php?id=223)
- Gibbs, G. (2010a, June 20). Grounded theory - axial coding [Video file]. Retrieved from [https://www.youtube.com/watch?v=s65aH6So\\_zY](https://www.youtube.com/watch?v=s65aH6So_zY)
- Gibbs, G. (2010b, June 11). Grounded theory - core elements. part 1 [Video file]. Retrieved from [https://www.youtube.com/watch?v=4SZDTp3\\_New](https://www.youtube.com/watch?v=4SZDTp3_New)
- Gibbs, G. (2010c, June 19). Grounded theory - core elements. part 2 [Video file]. Retrieved from [https://www.youtube.com/watch?v=dbntk\\_xeLHA](https://www.youtube.com/watch?v=dbntk_xeLHA)
- Gibbs, G. (2010d, June 19). Grounded theory - line-by-line coding [Video file]. Retrieved from [https://www.youtube.com/watch?v=Dfd\\_U-24egg](https://www.youtube.com/watch?v=Dfd_U-24egg)
- Gibbs, G. (2010e, June 19). Grounded theory - open coding part 1 [Video file]. Retrieved from [https://www.youtube.com/watch?v=gn7Pr8M\\_Gu8](https://www.youtube.com/watch?v=gn7Pr8M_Gu8)
- Gibbs, G. (2010f, June 19). Grounded theory - open coding part 2 [Video file]. Retrieved from [https://www.youtube.com/watch?v=vi5B7Zo0\\_OE](https://www.youtube.com/watch?v=vi5B7Zo0_OE)
- Gibbs, G. (2010g, June 19). Grounded theory - open coding part 3 [Video file]. Retrieved from <https://www.youtube.com/watch?v=n-EomYWkxcA>
- Gibbs, G. (2010h, June 20). Grounded theory - open coding part 4 [Video file]. Retrieved from <https://www.youtube.com/watch?v=AwmDRh5I7ZE>
- Gibbs, G. (2010i, June 20). Grounded theory - selective coding [Video file]. Retrieved from <https://www.youtube.com/watch?v=w9BMjO7WzmM>
- Gibbs, G. (2014, January 22). The nature of social research [Video file]. Retrieved from <https://www.youtube.com/watch?v=pQ4RAHXtvS0>
- Gibbs, G. (2015, May 6). Discourse analysis part 2: Foucauldian approaches [Video file]. Retrieved from [https://www.youtube.com/watch?v=E\\_ffCsQx2Cg](https://www.youtube.com/watch?v=E_ffCsQx2Cg)
- Gilbert, D. T., & Malone, P. S. (1995). The correspondence bias. *Psychological Bulletin*, 117(1), 21-38. doi:10.1037/0033-2909.117.1.21

- Gobierno de España. (2013). *Estrategia de ciberseguridad nacional 2013* [Spanish cybersecurity strategy 2013] .Presidencia del Gobierno. Departamento de Seguridad Nacional. Retrieved from <http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf>
- Golby, J. (2015, September 2). A teenager has accidentally shot himself dead while taking a selfie. *Vice*. Retrieved from [http://www.vice.com/en\\_uk/read/houston-teen-dies-taking-an-instagram-selfie-with-a-gun-or-how-selfies-will-kill-us-all-505](http://www.vice.com/en_uk/read/houston-teen-dies-taking-an-instagram-selfie-with-a-gun-or-how-selfies-will-kill-us-all-505)
- Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. California: Stanford University Press.
- Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2), 243-249.
- Grabosky, P., & Duffield, G. (2001, March). The psychology of fraud. *Trends and Issues in Crime and Criminal Justice*, 1-6. Retrieved from <http://www.aic.gov.au/>
- Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.), *Crime and the internet* (pp. 29-43). London: Routledge.
- Grasmick, H. G., Tittle, C. R., Bursik, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of gottfredson and hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, 30(1), 5-29. doi:10.1177/0022427893030001002
- Guglielmo, S. S. (2015). Cognitive distortion: Propositions and possible worlds. *Journal of Rational - Emotive and Cognitive - Behavior Therapy*, 33(1), 53-77. doi:10.1007/s10942-014-0202-7
- Haraway, D. (1991). *Simians, cyborgs and women: The reinvention of nature*. London: Free Association.
- Harrison, C. (2006). Cyberspace and child abuse images: A feminist perspective. *Affilia*, 21(4), 365-379. doi:10.1177/0886109906292313
- Hayles, K. (2010). What does it mean to be posthuman? In P. Nayar (Ed.), *the new media and cybercultures anthology*. Chichester, West Sussex, UK: Wiley-Blackwell.
- Helmreich, S. (2000). Flexible infections: Computer viruses, human bodies, nation-states, evolutionary capitalism. *Science, Technology, & Human Values*, 25(4), 472-491.
- Herrero Herrero, C. (2007). Criminología :(parte general y especial) [Criminology: (general and special part)].Madrid: Dykinson.
- Higgins, G. (2011). Value and choice: Examining their roles in digital piracy. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behavior* (pp. 141-154). CRC Press. doi:10.1201/b10718-13

- Higgins, G., Wolfe, S., & Marcum, C. (2011). Change of music piracy and neutralization. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behavior* (pp. 193-207). CRC Press. doi:10.1201/b10718-16
- Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology*, 9(3), 187-204. doi:10.1007/s10676-007-9143-5
- Hinduja, S. (2012). General strain, self-control, and music piracy. *International Journal of Cyber Criminology*, 6(1), 951-967.
- Hooley, T., Wellens, J., & Marriott, J. (2012). *What is online research?* London: Bloomsbury Publishing.
- IBM. (2015). IBM-statistical analysis software package- SPSS statistics. Retrieved from <http://www-03.ibm.com/software/products/en/spss-statistics>
- IC3. (2014). *2014 internet crime report*. FBI. Retrieved from [https://www.fbi.gov/news/news\\_blog/2014-ic3-annual-report](https://www.fbi.gov/news/news_blog/2014-ic3-annual-report)
- Ikea. (2015). Ikea catalogue 2016. Retrieved from [http://onlinecatalogue.ikea.com/GB/en/IKEA\\_Catalogue/](http://onlinecatalogue.ikea.com/GB/en/IKEA_Catalogue/)
- ILO. (2004). ISCO-international standard classification of occupations. Retrieved from <http://www.ilo.org/public/english/bureau/stat/isco/isco08/>
- INE. (2015a). Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares 2015 [Survey on equipment and use of Information and communication technologies in households 2015]. Retrieved from <http://www.ine.es/dynt3/inebase/es/index.htm?padre=2246&capsel=2247>
- INE. (2015b). Estadística de la enseñanza universitaria en España. Curso 2010-2011 [Statistics on university education in Spain. Course 2010-2011]. Retrieved from <http://www.ine.es/jaxi/tabla.do?path=/t13/p405/a2010-2011/I0/&file=02011.px&type=pcaxis&L=0>
- INE. (2015c). Población que usa internet (en los últimos tres meses) [Population using the internet (in the last three months)]. Retrieved from [http://www.ine.es/ss/Satellite?L=es\\_ES&c=INESeccion\\_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout&param3=1259924822888](http://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout&param3=1259924822888)
- Ingram, J. R., & Hinduja, S. (2008). Neutralizing music piracy: An empirical examination. *Deviant Behavior*, 29(4), 334-366. doi:10.1080/01639620701588131
- Internet Live Stats. (2015). Spain internet users. Retrieved from <http://www.internetlivestats.com/internet-users/spain/>
- ITU. (2014). *Measuring the information society report 2014*. (). Switzerland: International Telecommunication Union.

- Jewkes, Y., & Sharp, K. (2003). Crime, deviance and the disembodied self: Transcending the danger of corporeality. In Y. Jewkes (Ed.), *Dot.cons: Crime, deviance and identity on the internet* (pp. 1-14). Portland: Willan Publishing.
- Johnson, B. (2008, September 29). Cloud computing is a trap, warns GNU founder Richard Stallman. *The Guardian*. Retrieved from <http://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman>
- Juschka, D. M. (2009). *Political Bodies/Body politic: The semiotics of gender*. GB: Routledge Ltd
- Kasper, T. E., Short, M. B., & Milam, A. C. (2015). Narcissism and internet pornography use. *Journal of Sex & Marital Therapy*, 41(5), 481-486. doi:10.1080/0092623X.2014.931313
- Katz, J. E., & Aakhus, M. (2002). Conclusion: Making meaning of mobiles- A theory of *apparatchest*. In Authors (Eds.), *Perpetual contact: Mobile communication, public talk, private performance* (pp. 301-318). Cambridge: Cambridge University Press.
- Kipper, G., & Rampolla, J. (2012). *Augmented reality: An emerging technologies guide to AR*. Elsevier Science and Technology Books, Inc. Retrieved from [http://common.books24x7.com.libaccess.hud.ac.uk/book/id\\_47311/book.asp](http://common.books24x7.com.libaccess.hud.ac.uk/book/id_47311/book.asp)
- KPMG. (2007). *Profile of a fraudster survey 2007*. Switzerland: KPMG International. Retrieved from <http://www.kpmg.com/pl/en/issuesandinsights/articlespublications/pages/profile-of-a-fraudster-survey-2007.aspx>
- KPMG. (2011). *KPMG analysis of global patterns of fraud: Who is the typical fraudster?*. Switzerland: KPMG International. Retrieved from <https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/who-is-the-typical-fraudster.PDF>
- Kuni, V. (2007). Cyborg - communication - code - infection. *Third Text*, 21(5), 649-659. doi:10.1080/09528820701600178
- Lê, T., & Lê, Q. (2009). Critical discourse analysis: An overview. (pp. 3-15. In Lê, T., & Short, M. (Eds.). *Languages and linguistics: Critical discourse analysis: An interdisciplinary perspective*. New York, NY, USA: Nova.
- Leech, N. L., & Onwuegbuzie, A. J. (2009). A typology of mixed methods research designs. *Quality & Quantity*, 43(2), 265-275. doi:10.1007/s11135-007-9105-3
- Ley orgánica 2/1986, de 13 marzo, de fuerzas y cuerpos de seguridad [Organic act 2/1986, march 13th, of the security corps] (1986).
- Ley orgánica 10/1995, de 23 de noviembre, del código penal [Organic act 10/1995, November 23rd, of the criminal code] (1995).
- Ley orgánica 5/2010, de 22 de junio, por la que se modifica la ley orgánica 10/1995, de 23 de noviembre, del código penal [Organic act 5/2010, June 22nd, that modifies organic act 10/1995, November 23rd, of the criminal code] (2010).



- Ley orgánica 1/2015, de 30 de marzo, por la que se modifica la ley orgánica 10/1995, de 23 de noviembre, del código penal [Organic act 1/2015, march 30th, that modifies organic act 10/1995, november 23rd , of the criminal code]. (2015).
- Lessig, L. (2006). *Code: Version 2.0* (2nd ed.). New York: Basic Books.
- Lever-Mazzuto, K. (2012). Katz and aakhus' theory of apparatgeist: Students' perceptions of normative and non-normative behaviors for technology use. *Communication Teacher*, 26(2), 82-86. doi:10.1080/17404622.2011.643804
- Lipovetsky, G. (2005). *Hypermodern times*. Cambridge: Polity.
- Lipsman, A. (2014, August 8). Does snapchat's strength among millennials predict eventual mainstream success? Retrieved from <http://www.comscore.com/Insights/Blog/Does-Snapchats-Strength-Among-Millennials-Predict-Eventual-Mainstream-Success?>
- Madge, C., O'Connor, H., Wellens, J., Hooley, T. & Shaw, R. (2006). Exploring online research methods, incorporating TRI-ORM; an online research methods training programme for the social science community. Retrieved from <http://www.restore.ac.uk/orm/site/home.htm>
- Maeztu, D. (2011, January 18). Ataques DoS: ¿delito o forma de protesta?[DoS attacks: Crime or protest?]. Retrieved from <http://www.publico.es/ciencias/ataques-delito-o-forma-protesta.html>
- Maruna, S. (2001). *Making good: How ex-convicts reform and rebuild their lives*. Washington, D.C; London: American Psychological Association.
- Maruna, S., & Mann, R. E. (2006). A fundamental attribution error? rethinking cognitive distortions? *Legal and Criminological Psychology*, 11(2), 155-177. doi:10.1348/135532506X114608
- Marvel. (2015). Marvel AR app. Retrieved from <http://marvel.com/help/category/32>
- McAfee. (2014, Feb 4). Study reveals majority of adults share intimate details via unsecured digital devices. Retrieved from <http://www.mcafee.com/us/about/news/2014/q1/20140204-01.aspx>
- McMyler, B. (2007). Knowing at second hand. *Inquiry*, 50(5), 511-540. doi:10.1080/00201740701612390
- Mercer, J. (2012). Gay for pay: The internet and the economics of homosexual desire. In K. Ross (Ed.), *Handbooks in communication and media, volume 18: Handbook of gender, sex, and media* (pp. 535-551). Hoboken, NJ, USA: Wiley-Blackwell.
- Merton, R. K. (1968). *Social theory and social structure* (Enlarg ed.). New York; London: Free Press.
- Millard, D. (2015, August 27). Did Instagram bro hero Dan Bilzerian get his start thanks to his father's dirty money? *Vice*. Retrieved from <http://www.vice.com/read/did-instagram-bro-hero-dan-bilzerian-get-his-start-thanks-to-his-fathers-dirty-money-827>

- Miller, J. M., Wright, R. A., & Dannels, D. (2001). Is deviance "dead"? the decline of a sociological research specialization. *The American Sociologist*, 32(3), 43-59. doi: 10.1007/s12108-001-1027-2
- Ministerio del Interior. (2006). *Premio a la excelencia en la gestión pública 2006- centro de formación C.N.P Ávila* [Excellence award in public management 2006- education centre national police Ávila]. Retrieved from [http://www.policia.es/org\\_central/division\\_forma\\_perfe/premio\\_excelencia.pdf](http://www.policia.es/org_central/division_forma_perfe/premio_excelencia.pdf)
- Ministerio del Interior. (2013). *Avance de datos de cibercriminalidad 2013* [Cybercrime data advance 2013]. Ministerio del Interior. Retrieved from <http://www.interior.gob.es/documents/10180/1207668/Avance+datos+cibercriminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815>
- Miró Llinares, F. (2011). La oportunidad criminal en el ciberespacio: Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen [The criminal opportunity in cyberspace: Application and development of routine activity theory for the prevention of cybercrime]. *Revista Electrónica De Ciencia Penal y Criminología*, (13), 7:01-7:55. Retrieved from <http://criminnet.ugr.es/recpc/index.html>
- Moore, R. (2011). Digital file sharing: An examination of neutralization and rationalization techniques employed by digital file sharers. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behavior* (pp. 209-225) CRC Press. doi:doi:10.1201/b10718-17
- Moore, R., & McMullan, E. C. (2009). Neutralizations and rationalizations of digital piracy: A qualitative analysis of university students. *International Journal of Cyber Criminology*, 3(1), 441.
- Morgan, M., Coombes, L., & Connor, G. (2015). iAnorexic: Haraway's cyborg metaphor as ethical methodology. *Qualitative Research in Psychology*, 12(3), 233. doi:10.1080/14780887.2015.1008901
- NCA. (2015). National cyber crime unit. Retrieved from <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit>
- Newman, G. R., & Clarke, R. V. G. (2003). *Superhighway robbery: Preventing e-commerce crime*. Cullompton: Willan.
- INTECO, & Orange (2010). *Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles* [Study on security and privacy in the use of mobile services by Spanish minors]. Retrieved from [http://www.pantallasamigas.net/pdf/estudio\\_sobre\\_seguridad\\_y\\_privacidad\\_en\\_el\\_uso\\_de\\_los\\_servicios\\_moviles\\_por\\_los\\_menores\\_espanoles.pdf](http://www.pantallasamigas.net/pdf/estudio_sobre_seguridad_y_privacidad_en_el_uso_de_los_servicios_moviles_por_los_menores_espanoles.pdf)
- Schoepfer, A., & Piquero, A. (2006). Self-control, moral beliefs, and criminal activity. *Deviant Behavior*, 27(1), 51-71. doi:10.1080/016396290968326
- Público. (2013, October 30). Detenido un ultraderechista por los ataques a varios medios digitales [A far-rightist has been arrested because of the attacks on various digital media].

- Retrieved from <http://www.publico.es/actualidad/detenido-ultraderechista-ataques-varios-medios.html>
- QSR International. (2015). QSR-NVivo products. Retrieved from <http://www.qsrinternational.com/product>
- Randall, D. M., & Fernandes, M. F. (1991). The social desirability response bias in ethics research. *Journal of Business Ethics*, 10(11), 805-817. doi:10.1007/BF00383696
- Reeves, C. (2013). Fantasy depictions of child sexual abuse: The problem of ageplay in second life. *Journal of Sexual Aggression*, 19(2), 236-246. doi:10.1080/13552600.2011.640947
- Reiner, R. (2010). *The politics of the police* (4th ed.). Oxford: Oxford University Press.
- Ringrose, J., Gill, R., Livingstone, S., & Harvey, L. (2012). *A qualitative study of children, young people and 'sexting'*. NSPCC. Retrieved from <https://www.nspcc.org.uk/services-and-resources/research-and-resources/qualitative-study-sexting/>
- Rollins, J. (2015). Sexting cyberchildren: Gender, sexuality, and childhood in social media and law. *Sexuality & Culture*, 19(1), 57-71. doi:10.1007/s12119-014-9243-4
- Romero, E., Gómez-Fraguela, A., Luengo, Á., & Sobral, J. (2003). The self-control construct in the general theory of crime: An investigation in terms of personality psychology. *Psychology, Crime and Law*, 9(1), 61-86. doi:10.1080/10683160308142
- Rowe, M. (2008). *Introduction to policing*. London: SAGE.
- Ruiz Marull, D. (2015, July 5). Selfies extremos que llevan a la muerte [Extreme selfies leading to death]. *La Vanguardia*. Retrieved from <http://www.lavanguardia.com/sucesos/20150705/54433730328/selfies-muerte.html>
- Rusch, J. J. (n.d.). The "social engineering" of internet fraud. Retrieved from [http://www.isoc.org/inet99/proceedings/3g/3g\\_2.htm](http://www.isoc.org/inet99/proceedings/3g/3g_2.htm)
- Schofield, J. (2008, August 6). When google owns you.... your data is in the cloud. *The Guardian*. Retrieved from <http://www.theguardian.com/technology/blog/2008/aug/06/whengoogleepownsyouyourdata>
- Seigfried-Spellar, K., Lovely, R., & Rogers, M. (2011). Self-reported internet child pornography consumers. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behavior* (pp. 65-77) CRC Press. doi:doi:10.1201/b10718-8
- Servera, J. (2014a, July 21). ¿Puede twitter prevenir el crimen? [Can Twitter prevent crime?] *Criminología y Justicia*. Retrieved from <http://cj-worldnews.com/spain/index.php/es/>
- Servera, J. (2014b, June 17). Problemas de la aceleración tecnológica en criminología [Problems of the technological acceleration in criminology]. *Criminología y Justicia*. Retrieved from <http://cj-worldnews.com/spain/index.php/es/>

- Servera, J. (2015, September 8). El internet de las cosas va a cambiar la forma de prevenir el crimen [The internet of things is going to change the way of preventing crime]. *Criminología y Justicia*. Retrieved from <http://cj-worldnews.com/spain/index.php/es/>
- Sexual offences act 2003, c. 42 (2003).
- Silverman, D. (2010). *Doing qualitative research: A practical handbook* (3rd ed.). London: Sage.
- Skills Matter. (2014). Droidcon hackathon 2014|1st-2nd nov 2014 london. Retrieved from <https://skillsmatter.com/conferences/6337-droidcon-hackathon-2014>
- Snapchat. (2015). Snapchat. Retrieved from <https://www.snapchat.com/>
- Strassberg, D. S., McKinnon, R. K., Sustaíta, M. A., & Rullo, J. (2013). Sexting by high school students: An exploratory and descriptive study. *Archives of Sexual Behavior*, 42(1), 15-21. doi:10.1007/s10508-012-9969-8
- Sumner, C. (1994). *The sociology of deviance: An obituary*. Buckingham: Open University Press
- Sutherland, E. H. (1937). *The professional thief*. Chicago: The University of Chicago Press.
- Sutherland, E. H. (1983). *White collar crime (the uncut version)*. New Haven, CT: Yale University Press.
- Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22(6), 664-670. doi:10.2307/2089195
- The Open University. (2015). Distance learning courses and adult education. Retrieved from <http://www.open.ac.uk/>
- Tsatsou, P. (2012). Gender and sexuality in the internet era. In K. Ross (Ed.), *Handbooks in communication and media, volume 18 : Handbook of gender, sex, and media* (pp. 516-534). Hoboken, NJ, USA: Wiley-Blackwell, 2011.
- Turgeman-Goldschmidt, O. (2011). Identity construction among hackers. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behavior* (pp. 31-51) CRC Press. doi:doi:10.1201/b10718-6
- Turkle, S. (2005). *Second self : Computers and the human spirit*. Cambridge, MA, USA: MIT Press.
- Universidad Europea de Madrid. (2015). Universidad privada en Madrid [Private university in Madrid]. Retrieved from <http://universidadeuropea.es/en/>
- Universitat Oberta de Catalunya. (2015). Universitat oberta de Catalunya [Catalonia open university]. Retrieved from <http://www.uoc.edu/portal/en/index.html>
- Vicini, A., & Brazal, A. M. (2015). Longing for transcendence: Cyborgs and trans- and posthumans. *Theological Studies*, 76(1), 148-165. doi:10.1177/0040563914565308
- Wall, D. S. (2003). *Crime and the internet*. London: Routledge.

- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity.
- Wall, D. S. (2008a). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society*, 11(6), 861. doi:10.1080/13691180802007788
- Wall, D. S. (2008b). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, 22(1), 45-63. doi:10.1080/13600860801924907
- Wall, D. S. (2013). Policing identity crimes. *Policing and Society*, 23(4), 437-460. doi:10.1080/10439463.2013.780224
- Wells, J. J. (2014). Keep calm and remain human: How we have always been cyborgs and theories on the technological present of anthropology. *Reviews in Anthropology*, 43(1), 5-34. doi:10.1080/00938157.2014.872460
- Welsh, B. C., & Farrington, D. P. (2012). Crime prevention and public policy. In B. C. Welsh, & D. P. Farrington (Eds.), *The oxford handbook of crime prevention* (). Oxford University Press.
- Wellsmith, M. (2012). Preventing wildlife crime. *CJM : Criminal Justice Matters*, (90), 18. doi: 10.1080/09627251.2012.751219
- Wikström, P. H. (2006). Individuals, settings, and acts of crime: Situational mechanisms and the explanation of crime. In P. H. Wikström, & R. J. Sampson (Eds.), *The explanation of crime: Context, mechanisms and development* (pp. 61-107). Cambridge: Cambridge University Press.
- Wikström, P. H. (2010). Explaining crime as moral actions. In S. Hitlin, & S. Vaisey (Eds.), *Handbook of the sociology of morality* (pp. 211-239). New York: Springer. doi:10.1007/978-1-4419-6896-8\_12,
- Wikström, P. H., Oberwittler, D., Treiber, K., & Hardie, B. (2013). *Breaking rules: The social and situational dynamics of young people's urban crime*. Oxford: Oxford University Press
- Wikström, P. H., & Svensson, R. (2010). When does self-control matter? the interaction between morality and self-control in crime causation. *European Journal of Criminology*, 7(5), 395-410. doi:10.1177/1477370810372132
- Wikström, P. H., & Treiber, K. (2007). The role of self-control in crime causation: Beyond gottfredson and hirschi's general theory of crime. *European Journal of Criminology*, 4(2), 237-264. doi:10.1177/1477370807074858
- Wikström, P. H., & Treiber, K. (2009). Violence as situational action. *International Journal of Conflict and Violence*, 3(1), 75-96.
- Wikström, P. H., Tseloni, A., & Karlis, D. (2011). Do people comply with the law because they fear getting caught? *European Journal of Criminology*, 8(5), 401-420. doi:10.1177/1477370811416415

- Wilson, M. W. (2009). Cyborg geographies: Towards hybrid epistemologies. *Gender, Place & Culture*, 16(5), 499-516. doi:10.1080/09663690903148390
- Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407-427. doi:10.1177/147737080556056=20
- Yardley, L. (2000). Dilemmas in qualitative health research. *Psychology & Health*, 15(2), 215-228. doi:10.1080/08870440008400302
- Zizek, S. (2008). *The sublime object of ideology (the essential Zizek)*. London: Verso.
- Zizek, S. (2009). *The plague of fantasies (the essential Zizek)*. London: Verso.

## Annex 1: Online Survey

12/12/2015

Encuesta sobre ciber-delito

### Encuesta sobre ciber-delito

Estimado encuestado/a,

Le invitamos a formar parte de un estudio sobre ciber-delitos. Antes de que tome la decisión de participar es importante que conozca las razones por las que se lleva a cabo este estudio y lo que involucra. Por favor, tómese su tiempo y lea con detenimiento la siguiente información, pudiendo comentarla conmigo si lo desea. No dude en preguntar si hay algo que no queda lo suficientemente claro o necesita más información.

¿En qué consiste el estudio?

El propósito del presente estudio es comprender de qué manera reaccionamos y cómo nos sentimos en relación con el ciber-delito. Para lograr esto, realizaremos un pequeño cuestionario sobre su personalidad (por favor, conteste de manera veraz). Una vez hecho esto, le mostraremos una serie de situaciones ficticias relacionadas con el ciber-delito, que le pediremos que gradúe de acuerdo con su moralidad. Además, le preguntaremos sobre las maneras de justificar las situaciones que usted ha leído en los casos. El estudio se realiza como parte de una tesis doctoral para la University of Huddersfield (<http://www.hud.ac.uk/index.php>)

¿Por qué me han elegido?

Ha sido elegido de manera aleatoria

¿Debo participar?

Es decisión suya hacerlo o no hacerlo. En caso de que desee participar se le pedirá que acepte este consentimiento informado. Usted podrá en todo momento revocar su participación en el estudio sin ofrecer razón alguna. Su decisión de dejar de participar (o de no participar) no afectará al anonimato o confidencialidad de sus datos. Se trata de un estudio vinculado únicamente al ámbito universitario.

En caso de que desee revocar su consentimiento una vez haya comenzado a realizar el cuestionario, salga de éste sin pulsar el botón "enviar"

¿Qué tendría que hacer si decido participar?

Si decide participar, rellenar el siguiente cuestionario on-line.

Tardará aproximadamente unos 10-15 minutos en completarlo

¿Se revelará mi identidad?

No. Toda la información que se obtenga de este cuestionario se tratará con la más estricta confidencialidad

¿Qué pasará con la información que obtengan sobre mí?

Toda la información obtenida sobre usted se tratará de manera segura y cualesquiera datos identificativos se harán desaparecer para garantizar el anonimato. Se estima que en algún momento futuro, este estudio se publique en algún artículo o libro o se presente en conferencias. En caso de que esto ocurra, su información será tratada con la más estricta confidencialidad.

¿Con quién puedo contactar si tengo más preguntas?

Si tiene dudas o necesita más información, contacte con:

Jorge Ramiro Pérez Suárez  
E-Mail: [jorgeramiro.perez@uem.es](mailto:jorgeramiro.perez@uem.es)  
Twitter: @jramiroperez

O mi supervisor en la University of Huddersfield  
Dr. Bernard Gallagher  
E-Mail: [b.gallagher@hud.ac.uk](mailto:b.gallagher@hud.ac.uk)

Es importante que lea, comprenda y acepte el siguiente consentimiento. Su contribución a este estudio es absolutamente voluntaria y no está obligado/a a participar. En caso de necesitar más información, contacte con el investigador.

Para aceptar el consentimiento responda a las siguientes preguntas

\*Obligatorio

### Consentimiento

[https://docs.google.com/forms/d/1E7VVNiA3oyL01qFk8F6MrEVsNfrM9aWE\\_MU9I76T84/edit?uiiv=1](https://docs.google.com/forms/d/1E7VVNiA3oyL01qFk8F6MrEVsNfrM9aWE_MU9I76T84/edit?uiiv=1)

1/11

**1. He sido informado de la naturaleza y finalidad de esta investigación \****Selecciona todos los que correspondan.*☐ Marque en caso afirmativo**2. Presto mi consentimiento para participar \****Selecciona todos los que correspondan.*☐ Marque en caso afirmativo**3. Comprendo que puedo revocar mi consentimiento en cualquier momento y sin ningún tipo de razón \****Selecciona todos los que correspondan.*☐ Marque en caso afirmativo**4. Entiendo que la información recogida se mantendrá en condiciones seguras durante cinco años en la University of Huddersfield \****Selecciona todos los que correspondan.*☐ Marque en caso afirmativo**5. Entiendo que ninguna otra persona que no sea el investigador tendrá acceso a la información proporcionada. \****Selecciona todos los que correspondan.*☐ Marque en caso afirmativo**6. Entiendo que se garantiza mi anonimato y que ni mi identidad, ni datos que puedan llevar a mi identificación, serán recogidos o incluidos en algún informe \****Selecciona todos los que correspondan.*☐ Marque en caso afirmativo**Precuestionario**

Por favor, responda a las siguientes preguntas sobre usted

¡Adelante!

**7. i. ¿Cuál es su sexo?***Marca solo un óvalo.*☐ Hombre☐ Mujer**8. ii. ¿Qué edad tiene?**

Introduzca el número de años

**9. iii. ¿Cuál es su nacionalidad?**

En caso de seleccionar otro, por favor, especifique

*Selecciona todos los que correspondan.*☐ Español/a☐ Otro:



10. **iv. ¿Cuál es su profesión?**

Indique el sector al que pertenece

Marca solo un óvalo.

- ☐ Estudiante en edad escolar
- ☐ Estudiante universitario
- ☐ Desempleado (actualmente no estudia ni trabaja)
- ☐ Salud y bienestar
- ☐ Construcción y automóviles
- ☐ Educación, investigación e idiomas
- ☐ Legal
- ☐ Información, comunicación y finanzas
- ☐ Alimentación y hostelería
- ☐ Industria del metal, gas, aceite y minería
- ☐ Administrativo/a
- ☐ Fuerzas y Cuerpos de Seguridad Públicos, Seguridad Privada y militar
- ☐ Comercio y agricultura
- ☐ Transporte, logística, viajes y limpieza
- ☐ Directivo de empresa (CEO, altos cargos, etc.)
- ☐ Organizaciones No Gubernamentales

11. **v. ¿Ha sido usted (o alguien de su familia o allegados) afectado/a por el delito/víctima del delito (en cualesquiera de sus manifestaciones o formas) el último año?**

Independientemente de que haya sido puesto en conocimiento de las autoridades

Selecciona todos los que correspondan.

- ☐ Si
- ☐ No

**Cuestionario (Parte I)**

Por favor, responda a las siguientes preguntas de manera sincera. No existen respuestas buenas o malas. Es importante que responda a todas las preguntas

Todas las preguntas tienen cuatro opciones para responder. Se trata de una escala de 1-4, los valores son los siguientes:

- 1- Totalmente en desacuerdo
- 2- Algo en desacuerdo
- 3- Algo de acuerdo
- 4- Totalmente de acuerdo

Lea con mucho detenimiento los enunciados.

¡Adelante!

12. **1: A menudo actúo de manera impulsiva, sin pararme a pensar**

Marca solo un óvalo.

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

13. **2: Evito implicarme en proyecto que sé que serán difíciles***Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

14. **3: Me gusta ponerme a prueba haciendo cosas que son un poco arriesgadas***Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

15. **4: Si pudiera elegir, preferiría hacer cosas físicas, más que actividades mentales***Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

16. **5: Intento buscar lo mejor para mí, aun cuando eso signifique ponerles las cosas difíciles a otros***Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

17. **6: Pierdo los estribos con bastante facilidad***Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

18. **7: No dedico mucho tiempo ni esfuerzo a planificar el futuro***Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

19. **8: Cuando las cosas se complican tiendo a abandonarlas***Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

20. **9: Hago cosas arriesgadas sólo para pasarlo bien***Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

21. **10: Casi siempre me siento mejor cuando estoy en movimiento que cuando estoy pensando**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

22. **11: La verdad es que no me preocupa mucho por otras personas cuando tienen problemas**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

23. **12: Cuando estoy enfadado con una persona, me apetece hacer o decir cosas que le hieran, más que dialogar con ella y explicarle por qué estoy enfadado**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

24. **13: Me gusta hacer cosas que me den placer aquí y ahora, aunque me puedan traer problemas más tarde**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

25. **14: Siempre que puedo, evito hacer tareas difíciles que me obliguen a esforzarme mucho**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

26. **15: Para mí son más importantes la aventura y la diversión que la seguridad**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

27. **16: Prefiero salir y hacer cosas, más que leer o pensar sobre ideas abstractas**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

28. **17: Si lo que yo hago molesta a otras personas, ese es su problema, no mío**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

29. **18: Cuando estoy enfadado de verdad, es mejor para las otras personas que no se me acerquen mucho**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

30. **19: Me preocupa más lo que pueda sucederme a corto plazo que lo que pueda ocurrirme en el futuro**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

31. **20: Las cosas de la vida que más me gustan son las cosas que resultan fáciles y que dan placer**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

32. **21: Algunas veces me parece divertido hacer cosas que luego pueden traerme problemas**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

33. **22: Parece que tengo más necesidad de actividad física que la mayoría de la gente de mi edad**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

34. **23: Intentaré hacer las cosas que quiero, aunque así cause problemas a otras personas**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

35. **24: Cuando estoy muy en desacuerdo con una persona, me resulta difícil hablar tranquilamente con ella sin alterarme**  
*Marca solo un óvalo.*

	1	2	3	4	
Totalmente en desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Totalmente de acuerdo

### Cuestionario (Parte II)

A continuación va a leer una serie de pequeñas situaciones ficticias. Posteriormente deberá responder una serie de preguntas sobre lo ocurrido en éstas, así como su percepción de algunos elementos.

Lea con detenimiento las situaciones y las preguntas y conteste, por favor, con la más absoluta sinceridad.

¡Adelante!

36. **Caso 1: "Susana quiere ver la última película de los X-Men. Ella prefiere hacerlo desde casa. El cine cuesta 9 € lo que le parece caro para su ajustado presupuesto estudiantil. Es por ello que se baja la película de una página de descargas de Internet y la ve en el salón de su casa" Pregunta 1: ¿Harias tú lo mismo que Susana?**

De 0-10 (siendo 0 absoluto desacuerdo, siendo 10 absoluto acuerdo)

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Absoluto desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absoluto acuerdo

37. **Pregunta 2: ¿Cómo de moralmente reprochable crees que es la actuación de Susana?**

0-10 (siendo 0 nada inmoral, siendo 10 absolutamente inmoral)

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Nada inmoral	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absolutamente inmoral

38. **Pregunta 3: En caso de hacerlo (ponte en la situación de Susana) ¿Qué te dirías a ti mismo o a los otros para justificar lo que has hecho?**

Selecciona todos los que correspondan.

- ☐ No es justificable
- ☐ No he hecho nada malo/No he cometido ningún delito
- ☐ No es culpa mía/Es culpa de los demás
- ☐ Es culpa de la víctima (la persona perjudicada por mis actos, la empresa perjudicada por mis actos, etc.)/Se lo tiene merecido
- ☐ Todo el mundo lo hace
- ☐ No me quedaba otra opción
- ☐ Estoy en mi derecho de hacerlo
- ☐ No pasa nada porque, de vez en cuando, haga algo delictivo/malo/incorrecto

39. **Caso 2: "Pedro y Adela salían juntos. Adela solía mandarle a Pedro fotografías suyas sugerentes a través del correo y la mensajería acompañada de mensajes muy picantes. Un día, Pedro descubre que Adela tiene un amante, por lo que decide vengarse de ella enviando las fotografías de Adela a sus amigos a través de las redes sociales y el e-mail, así como colgarlas en internet" Pregunta 4: ¿Harias tú lo mismo que Pedro?**

De 0-10 (siendo 0 absoluto desacuerdo, siendo 10 absoluto acuerdo)

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Absolutamente desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absolutamente de acuerdo

40. **Pregunta 5: ¿Cómo de moralmente reprochable crees que es la actuación de Pedro?**

0-10 (siendo 0 nada inmoral, siendo 10 absolutamente inmoral)

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Nada inmoral	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absolutamente inmoral

41. **Pregunta 6: En caso de hacerlo (ponte en la situación de Pedro) ¿Qué te dirías a ti mismo o a los otros para justificar lo que has hecho?**

*Selecciona todas las que correspondan.*

- ☐ No es justificable
- ☐ No he hecho nada malo/No he cometido ningún delito
- ☐ No es culpa mía/Es culpa de los demás
- ☐ Es culpa de la víctima (la persona perjudicada por mis actos, la empresa perjudicada por mis actos, etc.)/Se lo tiene merecido
- ☐ Todo el mundo lo hace
- ☐ No me quedaba otra opción
- ☐ Estoy en mi derecho de hacerlo
- ☐ No pasa nada porque, de vez en cuando, haga algo delictivo/malo/incorrecto

42. **Caso 3: "Juan tiene un compañero de clase al que todo el mundo llama "Chapi, El Chepas" del que la gente suele reírse en el colegio debido a su apariencia personal. Juan decide crear un perfil falso en una red social con el nombre "Chapi, El Chepas". En ese perfil se dedica a subir caricaturas y fotografías retocadas de su compañero de clase (siempre ofensivas) y publicar estados y comentarios falsos (siempre hirientes)" Pregunta 7: ¿Habrías tú lo mismo que Juan?**

De 0-10 siendo 0 absoluto desacuerdo, siendo 10 absoluto acuerdo

*Marca solo un óvalo.*

	0	1	2	3	4	5	6	7	8	9	10	
Absoluto desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absoluto acuerdo

43. **Pregunta 8: ¿Cómo de moralmente reproachable crees que es la actuación de Juan?**

De 0-10 (siendo 0 nada inmoral, siendo 10 absolutamente inmoral)

*Marca solo un óvalo.*

	0	1	2	3	4	5	6	7	8	9	10	
Nada inmoral	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absolutamente inmoral

44. **Pregunta 9: En caso de hacerlo (ponte en la situación de Juan) ¿Qué te dirías a ti mismo o a los otros para justificar lo que has hecho?**

*Selecciona todas las que correspondan.*

- ☐ No es justificable
- ☐ No he hecho nada malo/No he cometido ningún delito
- ☐ No es culpa mía/Es culpa de los demás
- ☐ Es culpa de la víctima (la persona perjudicada por mis actos, la empresa perjudicada por mis actos, etc.)/ Se lo tiene merecido
- ☐ Todo el mundo lo hace
- ☐ No me quedaba otra opción
- ☐ Estoy en mi derecho de hacerlo
- ☐ No pasa nada porque, de vez en cuando, haga algo delictivo/malo/incorrecto

45. **Caso 4: "Saray es una joven de 16 años que, a través de una red social, se hace amiga de un hombre de 31 años llamado Bad\_Wolf y comienzan una relación de tintes sexuales. Un día Bad\_Wolf pide a Saray que le envíe unas fotografías suyas desnuda. Saray está de acuerdo y lo hace" Pregunta 10: ¿Harias tú lo mismo que Saray?**

De 0-10 siendo 0 absoluto desacuerdo, siendo 10 absoluto acuerdo

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Absoluto desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absoluto acuerdo

46. **Pregunta 11: ¿Cómo de moralmente reproachable crees que es la actuación de Saray?**

De 0-10 siendo 0 nada inmoral, siendo 10 absolutamente inmoral

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Nada inmoral	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absolutamente inmoral

47. **Pregunta 12: ¿En caso de hacerlo (ponte en la situación de Saray) ¿Qué te dirías a ti mismo o a los otros para justificar lo que has hecho?**

Selecciona todos los que correspondan.

- ☐ No es justificable
- ☐ No he hecho nada malo/No he cometido ningún delito
- ☐ No es culpa mía/Es culpa de los demás
- ☐ Es culpa de la víctima (la persona perjudicada por mis actos, la empresa perjudicada por mis actos, etc.)/Se lo tiene merecido
- ☐ Todo el mundo lo hace
- ☐ No me quedaba otra opción
- ☐ Estoy en mi derecho de hacerlo
- ☐ No pasa nada porque, de vez en cuando, haga algo delictivo/malo/incorrecto

48. **Caso 5: "Alfredo es un hombre de 26 años. Sin embargo, en internet finge ser una atractiva soltera rusa llamada Natasha buscando casamiento en España. Para esto se dedica a enviar e-mails y mensajes a receptores aleatorios, diciéndoles que les ama y que Natasha quisiera casarse con ellos. Además, les pide dinero para poder gestionar el pasaporte y viajar a conocer a su futuro marido. Algunas personas ya han enviado dinero. " Pregunta 13: ¿Harias tú lo mismo que Alfredo?**

De 0-10 siendo 0 absoluto desacuerdo, siendo 10 absoluto acuerdo

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Absoluto desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absoluto acuerdo

49. **Pregunta 14: ¿Cómo de moralmente reproachable crees que es la actuación de Alfredo?**

siendo 0 nada inmoral, siendo 10 absolutamente inmoral

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Nada inmoral	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absolutamente inmoral



50. **Pregunta 15: ¿En caso de hacerlo (ponte en la situación de Alfredo) , qué te dirías a ti mismo o a los otros para justificar lo que has hecho?**

*Selecciona todas las que correspondan.*

- ☐ No es justificable
- ☐ No he hecho nada malo/No he cometido ningún delito
- ☐ No es culpa mía/Es culpa de los demás
- ☐ Es culpa de la víctima (la persona perjudicada por mis actos, la empresa perjudicada por mis actos, etc.)/Se lo tiene merecido
- ☐ Todo el mundo lo hace
- ☐ No me quedaba otra opción
- ☐ Estoy en mi derecho de hacerlo
- ☐ No pasa nada porque, de vez en cuando, haga algo delictivo/malo/incorrecto

51. **Caso 6: "Tomás está enamorado en secreto de su compañera de trabajo Débora. Diariamente le envía mensajes de amor desde una cuenta de e-mail falsa bajo el nombre "Tu admirador secreto". Tomás también ha creado una página web llamada [www.DeboraTeDevoraba.es](http://www.DeboraTeDevoraba.es) donde se dedica a subir fotografías de Débora obtenidas sin su permiso y cartas de amor. Débora está muy asustada y preocupada. " Pregunta 16 : ¿Harías tú lo mismo que Tomás?**

De 0-10 siendo 0 absoluto desacuerdo, siendo 10 absoluto acuerdo

*Marca solo un óvalo.*

	0	1	2	3	4	5	6	7	8	9	10	
Absoluto desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absoluto acuerdo

52. **Pregunta 17: ¿Cómo de moralmente reproachable crees que es la actuación de Tomás?**

De 0-10 siendo 0 nada inmoral, siendo 10 absolutamente inmoral

*Marca solo un óvalo.*

	0	1	2	3	4	5	6	7	8	9	10	
Nada inmoral	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absolutamente inmoral

53. **Pregunta 18: ¿En caso de hacerlo (ponte en la situación de Tomás) ¿Qué te dirías a ti mismo o a los otros para justificar lo que has hecho?**

*Selecciona todas las que correspondan.*

- ☐ No es justificable
- ☐ No he hecho nada malo/No he cometido ningún delito
- ☐ No es culpa mía/Es culpa de los demás
- ☐ Es culpa de la víctima (la persona perjudicada por mis actos, la empresa perjudicada por mis actos, etc.)/Se lo tiene merecido
- ☐ Todo el mundo lo hace
- ☐ No me quedaba otra opción
- ☐ Estoy en mi derecho de hacerlo
- ☐ No pasa nada porque, de vez en cuando, haga algo delictivo/malo/incorrecto



54. **Caso 7: "Rafa se acaba de mudar a su nuevo piso en Madrid. Está todo listo menos la Wi-Fi, parece que la instalación se demora un poco. Buscando entre las redes, descubre una red abierta de mucha potencia llamada "Chuqui\_2C" perteneciente a un vecino. Decide conectarse a esta red hasta que la conexión esté lista" Pregunta 19: ¿Harías tú lo mismo que Rafa?**

De 0-10 siendo 0 absoluto desacuerdo, siendo 10 absoluto acuerdo

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Absoluto desacuerdo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absoluto acuerdo

55. **Pregunta 20: ¿Cómo de moralmente reprochable crees que es la actuación de Rafa?**

De 0-10 siendo 0 nada inmoral, siendo 10 absolutamente inmoral

Marca solo un óvalo.

	0	1	2	3	4	5	6	7	8	9	10	
Nada inmoral	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Absolutamente inmoral

56. **Pregunta 21: En caso de hacerlo (ponte en la situación de Rafa) ¿Qué te dirías a ti mismo o a los otros para justificar lo que has hecho?**

Selecciona todos los que correspondan.

- ☐ No es justificable
- ☐ No he hecho nada malo/No he cometido ningún delito
- ☐ No es culpa mía/Es culpa de los demás
- ☐ Es culpa de la víctima (la persona perjudicada por mis actos, la empresa perjudicada por mis actos, etc.)
- ☐ Todo el mundo lo hace
- ☐ No me quedaba otra opción
- ☐ Estoy en mi derecho de hacerlo
- ☐ No pasa nada porque, de vez en cuando, haga algo delictivo/malo/incorrecto

**¡Enhorabuena!**

Ya ha finalizado la encuesta. ¡Muchísimas gracias por su tiempo!

No olvide pulsar el botón "enviar" para que todas las respuestas queden guardadas

Con la tecnología de



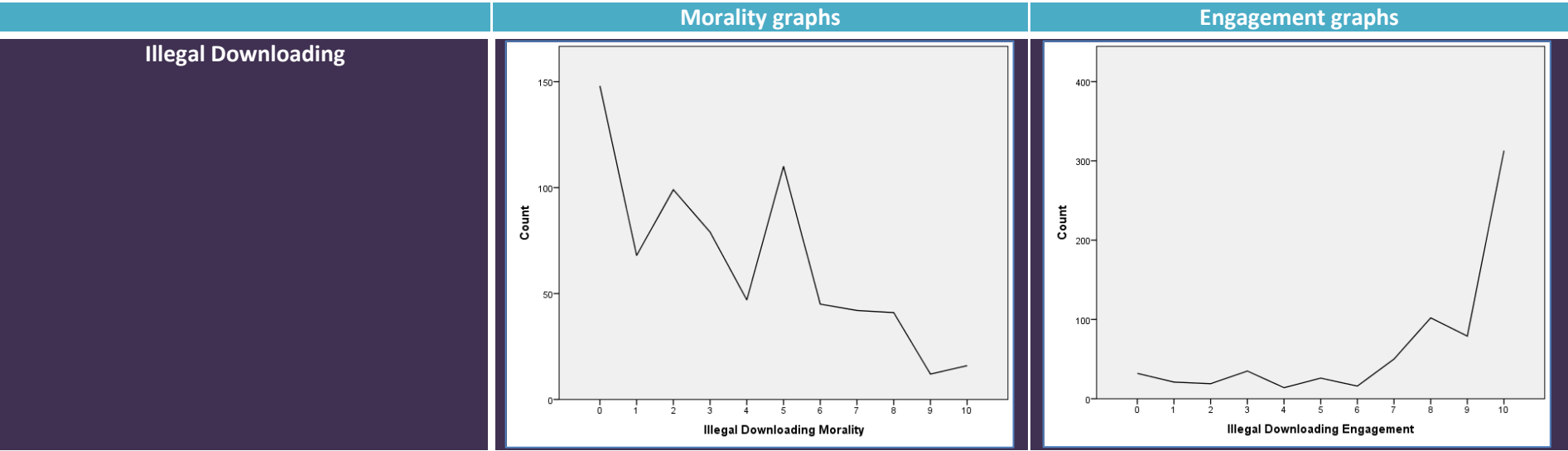
## Annex 2: Vignettes

	Vignette	Questions
Illegal Downloading	Jill wants to watch the latest X-Men movie, but she prefers to stay at home, also the cinema is 6 £ which she finds very expensive for her student budget. Jill decides to download a pirate copy of the movie on the Internet and watches it at home.	<p>1.-Would you do what Jill did? 0-10 (being 0 absolute disagreement, being 10 absolute agreement)</p> <p>2.- How morally wrong do you think Jill's actions are? 0-10 (being 0 absolutely not immoral, being 10 absolutely immoral)</p> <p>3.-In the case of case of doing it (place yourself in Jill's shoes). What would you tell yourself or others to justify what you have done?</p>
Revenge Porn	Peter and Susan were going out. Susan used to send suggestive pictures of herself via e-mail and messages accompanied by saucy messages. One day Peter discovers Susan is having an affair and he decides to take revenge on her by sending her pictures and messages to his friends via social networks and e-mail, as well as posting them on the internet.	<p>4.- Would you what Peter did? 0-10 (being 0 absolute disagreement, 10 absolute agreement)</p> <p>5.- How morally wrong do you think Peter's actions are? 0-10 (being 0 absolutely not immoral, 10 absolutely immoral)</p> <p>6.- In the case of doing it, what would you tell yourself (place yourself in Peter's shoes) or others to justify what you have done?</p>
Cyberbullying	John has a class-mate that people call Pete Pimple. He is usually mocked at school because of his personal appearance. John decides to create a fake social network profile with the name of Pete Pimple. In that profile John posts caricatures of Pete and doctored pictures (always offensive) as well as fake statuses and comments (always harmful).	<p>7.-Would you what John did? 0-10 (being 0 absolute disagreement, 10 absolute agreement)</p> <p>8.- How morally wrong do you think John's actions are? 0-10 (being 0 absolutely not immoral, absolutely immoral)</p> <p>9.- In the case of doing it, what would you tell yourself (place yourself in John's shoes) or others to justify what you have done?</p>

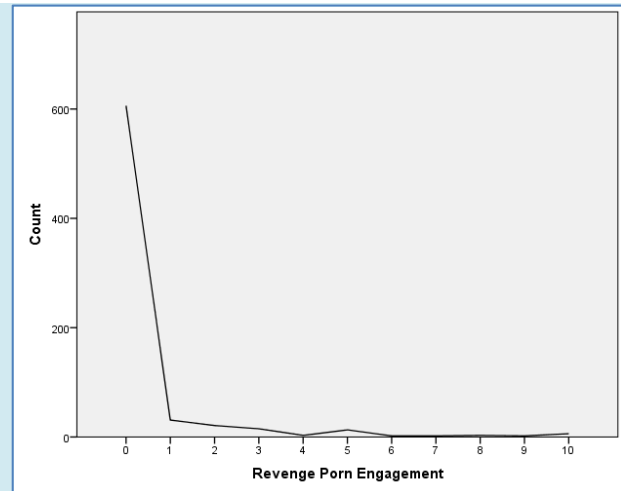
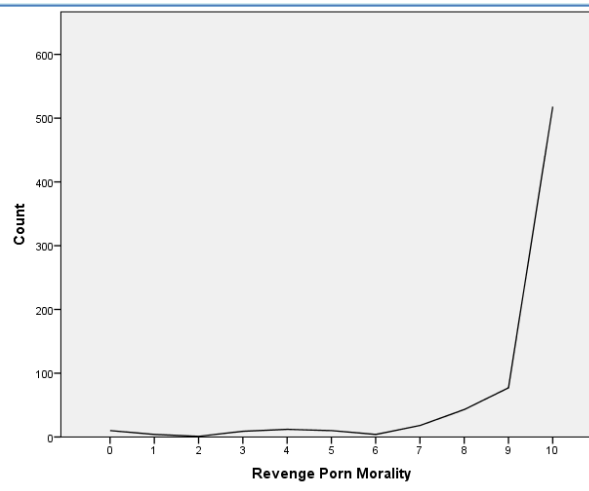
<b>Sexting</b>	Gena is a 16 year old that, by using social networks, has befriended a 31 year old man called Bad_Wolf and has started a sexual relationship. One day Bad_Wolf asks Gena for some naked pictures of herself. Gena agrees and does it.	10.- Would you do what Gena did? 0-10 (being 0 absolutely disagreement, 10 absolute agreement) 11.- How morally wrong do you think Gena's action are? 0-10 (being 0 absolutely not immoral, 10 absolutely immoral) 12.- In the case of doing it (place yourself in Gena's shoes). What would you tell yourself or others to justify what you have done?
<b>Cyberfraud</b>	Alfred is 26 year old man, yet on the internet he pretends to be an attractive Russian splinter called Natasha looking for marriage in the UK. He sends e-mails and fake pictures to random people telling them how much "she" loves them and that "she" would like to marry them. Also, "she" asks for money in advance in order to get a passport done and travel to meet "her" future husband. Some people have already sent him money.	13.- Would you do what Alfred did? 0-10 (being 0 absolute disagreement, 10 absolute agreement) 14.- How morally wrong do you think Alfred's actions are? 0-10 (0 absolutely not immoral, 10 absolutely immoral) 15.- In case of doing it, what would you tell yourself (place yourself in Alfred's shoes) or others to justify what you have done?
<b>Cyberstalking</b>	Tom is secretly in love with his work-mate Deborah. He constantly sends her e-mails and texts from a fake e-mail account singed as "Your secret admirer". Tom has created a web-page called "DeborahldDevourYou.com" where he posts pictures of her taken without permission and love letters. Deborah feels very uncomfortable and scared about this.	16.- Would you do the Tom did? 0-10 (0 absolute agreement, 10 absolute disagreement) 17.- How morally wrong do you think Tom's actions are? 0-10 (0 absolutely not immoral, 10 absolutely immoral) 18.- In case of doing it, what would you tell yourself (place yourself in Tom's shoes) or others to justify what you have done?
<b>Wi-Fi Stealing</b>	Alistair just moved into his new flat in Liverpool. Everything is ready, but the Wi-Fi. The provider seems to delay the installation. Browsing the networks he finds and open and powerful Network called "Marty_2C", belonging to his neighbour. He decides to log on to this network whilst his connection is not ready.	19.-Would you do what Alistair did? 0-10 (0 absolute disagreement, 10 absolute agreement) 20.- How morally wrong do you think Alistair's actions are? 0-10 (0 absolutely not immoral, 10 absolute immoral) 21.-In case of doing it, what would you tell yourself (place yourself in Alistair's' shoes) or others to justify what you have done?

Annex 3: Vignette Graphs

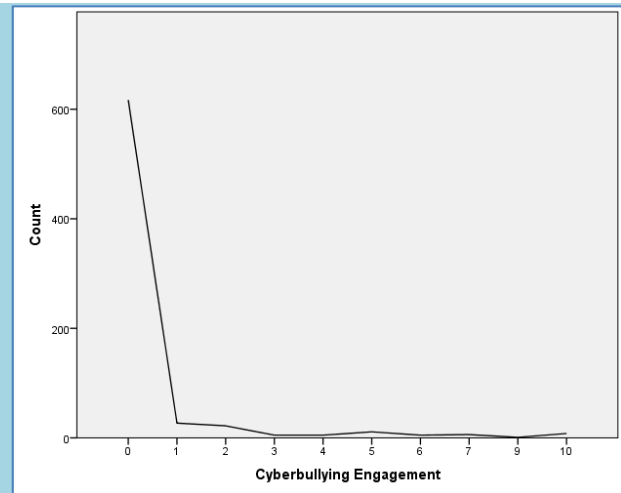
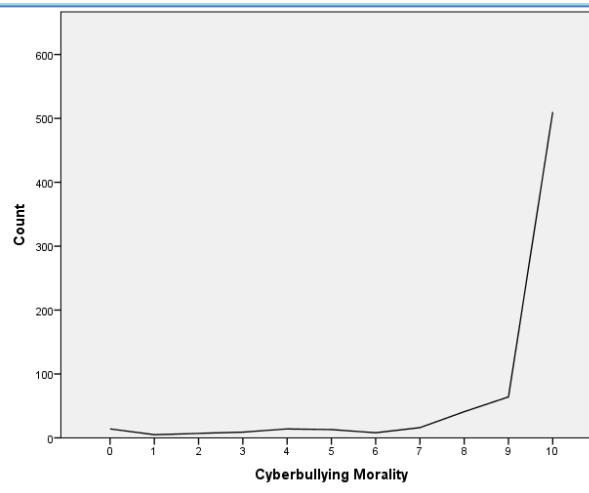
The vignettes coloured in a darker tone show a different distribution pattern.



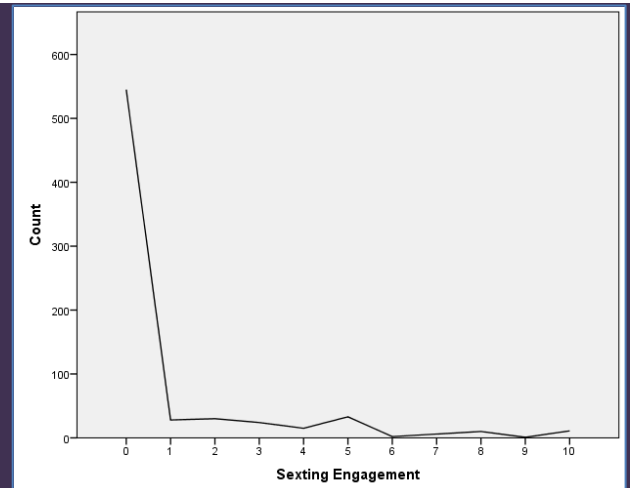
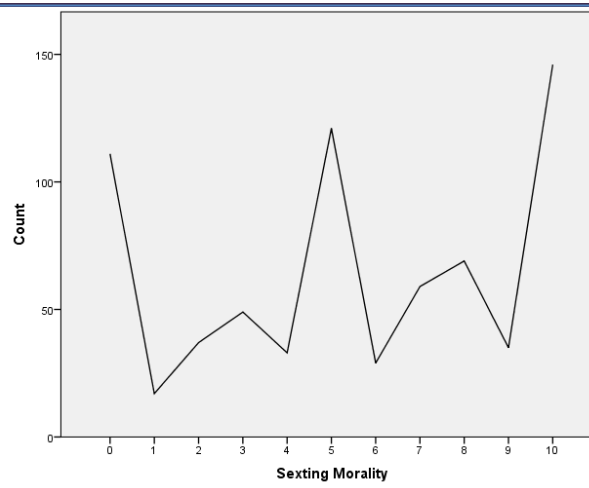
## Revenge Porn



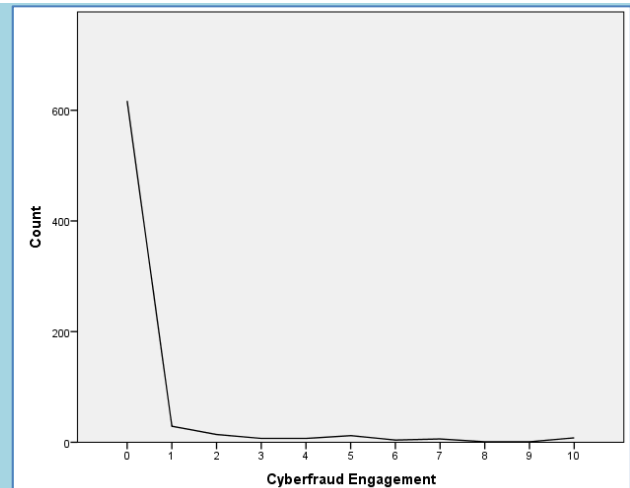
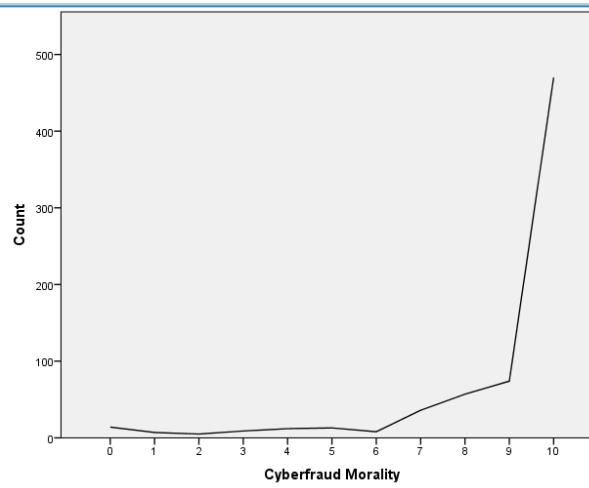
## Cyberbullying



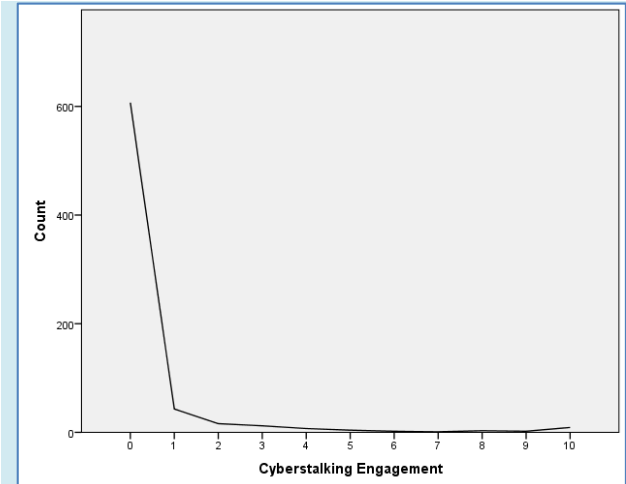
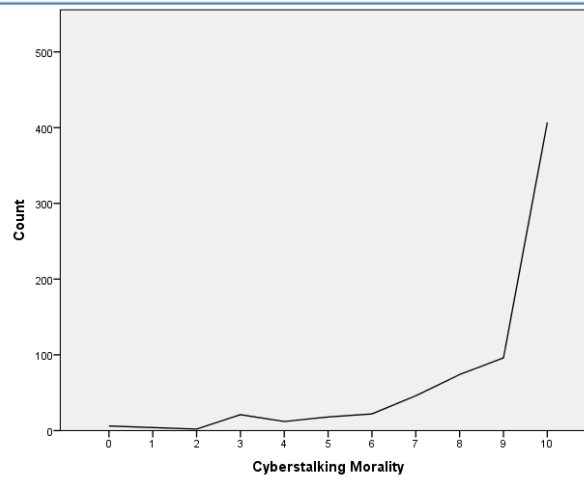
## Sexting



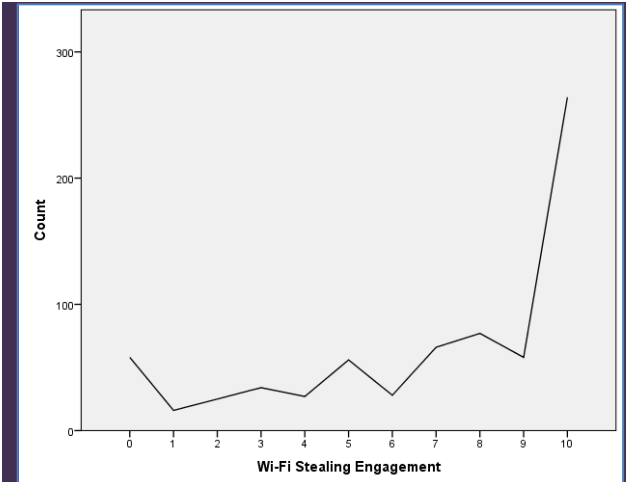
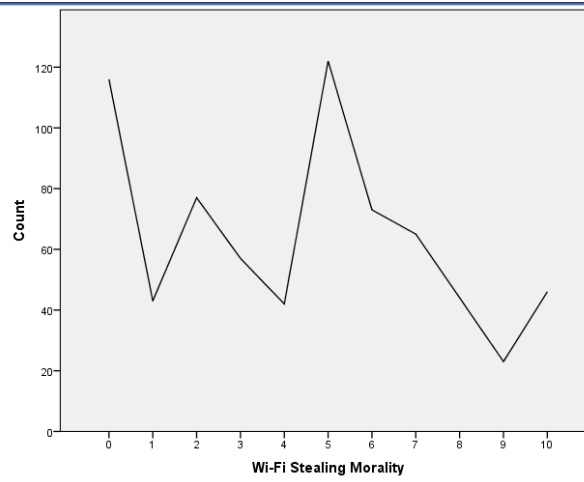
## Cyberfraud



## Cyberstalking



## Wi-Fi Stealing



#### Annex 4: Summary of Cases from Interviews with Law Enforcement Agents

Case List	Source	Name	Cybercrime	Investigation	Offender/s involved	Neutralisation	Special Features
C1	GCEX	"The Botnet"	Hacking: Creation of Zombie/slave networks	-Contact from software company - Reversing of malware -Forensics of infested hardware - Led to control panel in Spain -IP analysis	-3 (organised crime)	- Career Criminal/Professional	-Slovenian contacts
C2	GCEX	"The Social Network"	Prostitution/Soliciting via Social Networks	- Minor reveals illegal activity - Investigation of social networks -10 profiles investigated	- Minors: 15 -Adults: 10	- The robustness of heterosexual identity	-Minors involved -Excessive acquisitiveness of capitalist societies
C3	GCEX	"Phishing"	Cyberfraud: Bogus bank webpage Fake ID's Fake cards	-International investigation of Fake ID's -Following money trail -Bank surveillance	-Organised crime	-Career Criminal/Professional	- International Complexity



<b>C4</b>	PSEX	"Nannysex"	Peadophile ring/Child Pornography exchange community/Child abuse	-P2P exchanges -Investigation of IP's - Private message boards and chats	-+100 offenders - Mostly consumers, they reach one of the producers	-Fun/Game -Cognitive distortions	-Extreme public outrage -Gravest known paedophile ring in Spain
<b>C5</b>	PSEX	"The solitaire"	Bank Robbery aided by computer: <b>Not a valid cybercrime</b>	-Forensic investigation of computer	-The solitaire	-Not indicated	-Media repercussions
<b>C6</b>	PSEX	"The kid with the katana"	Murder of parents with sword: <b>Not a valid cybercrime</b>	-Forensic investigation of computer - Left a letter in computer	-Minor with psychopathology	-Not indicated	-Minor involved -Media outrage
<b>C7</b>	PSEX	"Information Breach"	Copy/Selling of confidential information: Disloyal employee practices	- Not Indicated	-Disgruntled employee	-Denial of injury - Capitalistic critique	Private Sector
<b>C8</b>	PSEX	"Ticket Scam"	Hacking of hard-drives in order to sell fake tickets for show	-General overview	-Not indicated	-Not indicated	Current case
<b>C9</b>	PSEX	"Breaking of e-mail confidentiality"	Hacking and spying company's mail accounts/ Disloyal competence/Security breaches	- General overview	- Not indicated	- Absence of a culture of privacy and security (neutralisation implicit)	Private Sector
<b>C10</b>	NPEX1	"Online gambling fraud"	Cyberfraud (including money laundering and ID fraud)	-Information about fraudulent company emerges online - Police contacts	-3 (family business)	- Career criminal/Professional - Denial of injury	-Polish and Swiss elements

				victims and offers legal actions - Investigation of fraudulent webpage			
<b>C11</b>	NPEX1	"Siglo XXI"	Hybrid fraud (Traditional+Cyberfraud): Creation of bogus webpages and magazines (usually relating to Police affairs) in order to obtain money from advertising	-The Police starts receiving complaints about aggressive tele-marketing schemes -Police starts investigation fake webpages -Police investigates fake companies -Police investigates fake magazines	- 52 (family business and organised crime) - Charismatic leader: creative, smart and lacking in remorse	- Career criminal/Professional	-Extremely complex multi-layered fraud -Never seen before
<b>C12</b>	NPEX1	"Nitro"	Uploading and performing illegal car races/Dangerous driving: <b>Not entirely a valid cybercrime</b>	-Police investigates a series of videos uploaded in Youtube -Police uncovers an unorganised network of illegal races in Mallorca	- 3 young people -A minor involved -They also had a Youtube for channel the uploading of their races	- Not indicated - Extreme vanity and low intellect are suggested in the organiser	-Minors involved
<b>C13</b>	NPEX2	"Police Porn Virus"	Ransomware/Cyberfraud: A virus stemming from	-The Police investigates an e-	-27 year old Russian	- Career Criminal/Professional	multi-national virus with

			porn pages infects computers and locks the O.S. asking form money in return. The virus impersonates the Spanish Police and accuses the victim of various crimes relating to watching porn	mail and UKASH account -The Police discovers a virus spreading internationally with “bullet-proof hosting”	-Wealthy life-style	-Denial of victim and injury	various versions depending on Country -Spreaded easily and quickly -Russian origin
<b>C14</b>	NPEX2	“Cryptolocker”	Ransomware/Cyberfraud: A virus encrypts a computer and needs a decryption key boagh from the black market	-The Police are investigating a related network of money laundering and top-up cards code trafficking	-Russian family -Risk-benefit oriented -False sense of security and anonymity	- Career criminal/Professional	Current
<b>C15</b>	NPEX2	“Anonymous”	Hacktivism/Defacement: Anonymous Spain (including splinter cells) start a campaign of national security breaches, defacement of political parties web-pages and personal privacy violations and DoS attacks	-Police investigates why Anonymous Spain could hold a grudge against certain specific people and reach a disgruntled employee -Police investigates the defacement of webapges and reach a splinter group	-A disgruntled private security employee and his “acolyte” (there is revenge component) - A splinter cell in Málaga -A group called sector404	- The Appeal to Higher Loyalties (The Anonymous cause and manifesto) - Fun/Game	-Minors involved

<b>C16</b>	NPEX2	"Latin hackteam"	Hacking/Defacement	-Police investigate a page that posts screenshots of different hacking and defacement activities	-2	-Denial of Injury	-South-American connections
<b>C17</b>	NPEX2	"Information ransom"	Information theft/Cyberfraud: A minor steals delicate information from a company and asks for a 2.500 € ransom	-Police follow an e-mail trail that leads to the minor's mother	- 1 minor: Introvert and extremely intelligent. He has done it before.	-Denial of injury -Denial of victim - Fun/Game (implicit neutralisation)	-Minors involved
<b>C18</b>	NPEX3	"Nannysex"	Paedophile ring/Child Pornography exchange community/Child abuse	-The Police investigates a paedophile ring -The Police discovers a paedophile using the name "Nannysex" on the Internet, demanding extreme COPINE 4 content -	-Offender Nannysex is not Spanish -A paedophile ring is discovered -3 other offenders are investigated	- Cognitive distortions - Fun/Game	-International collaboration -Minors involved -Gravest child abuse case in Spain (including babies) -Nannysex was a "monster" within the paedophile world
<b>C19</b>	NPEX3	"Cool Daddy"	Paedophile ring/Child Pornography exchange community/Child abuse/Child prostitution	-The Police investigates child sex abuse videos found at the	-1	-Absolute denial	-International component

				<p>"Deep Web", depicting sex with sex with children on a boat</p> <p>-The Police investigates an e-mail address referring to someone called "Cool Daddy"</p> <p>-The Police investigates a boat appearing on the video</p> <p>-The Police investigates a bogus company</p>			
<b>C20</b>	NPEX3	"The Chameleon"	Cybergrooming and sextortion	<p>-The victim reports the crime to the police</p>	<p>-The offender blackmails the girls and sets a quota of sex pictures</p> <p>- He was a serial offender using several on-line identities (The Chameleon). He used dozens of e-mails</p> <p>-250 victims</p>	-Victim's Fault	-Sexual blackmail has profound effects on the adolescent's psyche

## Endnotes: Original Excerpts in Spanish

<sup>i</sup> El tercer delito más lucrativo a nivel mundial.

<sup>ii</sup> La ciberseguridad es una necesidad de nuestra sociedad y de nuestro modelo económico.

<sup>iii</sup> el objetivo es conectar a los objetos que nos rodean con las personas, y del mismo modo, conectar los objetos unos con otros.

<sup>iv</sup> Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal.

<sup>v</sup> El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento ...

<sup>vi</sup> El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor...

<sup>vii</sup> Por otra parte, la extensión de la utilización de Internet y de las tecnologías de la información y la comunicación con fines sexuales contra menores ha evidenciado la necesidad de castigar penalmente las conductas que una persona adulta desarrolla a través de tales medios para ganarse la confianza de menores con el fin de concertar encuentros para obtener concesiones de índole sexual.

<sup>viii</sup> También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeran, poseyeran o facilitaran programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

<sup>ix</sup> 197.3 El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

<sup>x</sup> Pedro y Adela salían juntos. Adela solía mandarle a Pedro fotografías suyas sugerentes a través del correo y la mensajería acompañada de mensajes muy picantes. Un día, Pedro descubre que Adela tiene un amante, por lo que decide vengarse de ella enviando las fotografías de Adela a sus amigos a través de las redes sociales y el e-mail, así como colgarlas en internet.

<sup>xi</sup> Saray es una joven de 16 años que, a través de una red social, se hace amiga de un hombre de 31 años llamado Bad\_Wolf y comienzan una relación de tintes sexuales. Un día Bad\_Wolf pide a Saray que le envíe unas fotografías suyas desnuda. Saray está de acuerdo y lo hace.

<sup>xii</sup> Tomás está enamorado en secreto de su compañera de trabajo Débora. Diariamente le envía mensajes de amor desde una cuenta de e-mail falsa bajo el nombre "Tu admirador secreto". Tomás también ha creado una página web llamada [www.DeboraTeDevoraba.es](http://www.DeboraTeDevoraba.es) donde se dedica a subir fotografías de Débora obtenidas sin su permiso y cartas de amor. Débora está muy asustada y preocupada.

---

<sup>xiii</sup> Vamos, lo que está claro es que son profesionales y es de lo que viven o sea no tienen otra actividad no, es decir, eso es un complemento a....No no su forma de vida es esta.

<sup>xiv</sup> Es decir, esto es su forma de vida entonces bueno tienen unos igual son unos elevados conocimientos, hablan perfectamente en este caso hablaban tres y cuatro idiomas desde ruso, inglés, español, francés, ¿vale? O sea que tienen un aparte bueno las personas de Europa del este tienen un don para el tema de los idiomas. Entonces tienen una facilidad para el aprendizaje increíble, pero bueno al final no deja de ser una forma de vida.

<sup>xv</sup> El menor tiene unas habilidades informáticas muy elevadas, es una persona muy retraída vive en un pueblo muy pequeño de Asturias que lo que hay son vacas.

<sup>xvi</sup> Si t en tu país de origen vivías de una manera y has adquirido unos conocimientos con los cuales cuando llegas a aquí poniendo en marcha esos conocimientos eres capaz de tener una compensación económica rápida y muy elevada, poder tener un nivel de vida en el cual tu no podías ni imaginar en estando en tu país....pues lógicamente lo vas a realizar.

<sup>xvii</sup> es un poco remota la ciudad allí en Rusia. No había muchas posibilidades, yo creo que ni económicas ni nada, y claro esta salida gente que técnicamente es buena en informática, programando virus y demás pues una salida muy rentable a su habilidades porque el trabajo que te puede dar trabajar de ingeniero o de consultor informático allí en Rusia o los beneficios que te pueden dar una campaña de este tipo pues no tiene nada que ver.

<sup>xviii</sup> Buen producto.

<sup>xix</sup> Entonces claro que el engaño estaba bien pensado en el sentido en que la infección procedía de páginas web donde mostraban contenido pornográfico.

<sup>xx</sup> tenía un buen virus, porque no era detectado por parte de ningún anti-virus.

<sup>xxi</sup> es súper seguro para ellos porque en ese momento dice vale, si pues nada lo elimina todo o remotamente me conecto a mi servidor y elimino todo y me abres otro en otro sitio, es decir, son servicios muy seguros para los criminales.

<sup>xxii</sup> yo tengo un buen producto, quiero llegar a cuantas más gente mejor a lo largo de todo el mundo. Entonces, ¿Qué forma puedo hacer?. Que es algo que visita todo el mundo, pues páginas de pornografía infantil, perdón, de pornografía, no de pornografía infantil de pornografía. Entonces si distribuyo este buen producto en páginas de pornografía que puede visitar un alemán, un chino, un español, un británico quien sea, pues bueno lo que tengo que hacer luego es dar un mensaje creíble a esas personas.

<sup>xxiii</sup> es la madre de todos los fraudes, sinceramente (en voz baja un grandísimo hijo de puta) yo de verdad los he cogido cariño, porque ha sido tan brutal y tan perfeccionada y todo tan estudiado, que jamás había visto yo cosas más perfectas, estafador más digno de admirar que este hombre, para mí va a ser la investigación de mi vida.

<sup>xxiv</sup> En este caso era una relación familiar, un clan, era una relación familiar porque siempre que hay una estructura organizativa criminal lo que hemos detectado es que hay una relación muy fuerte o una cercanía fuerte de confianza, generalmente se genera en las familias

<sup>xxv</sup> Entonces vimos que efectivamente la persona era un clan familiar ruso, asentado aquí, era el padre, el hijo, el hijo de la novia del padre y las novias de los dos hijos, o sea era, totalmente un clan cerrado de la familia, tenían este modo de vida y este modo de negocio.

<sup>xxvi</sup> evidentemente por el idioma y por la comunicación mucho más sencilla.

---

<sup>xxvii</sup> el perfil del estafador, es una persona sin escrúpulos, un ánimo desmedido de lucro y suelen ser personas muy inteligentes y muy ingeniosas y muy creativas, no porque , la verdad es que aunque te ríes de las argucias que utilizan para estafar.

<sup>xxviii</sup> Y bueno el perfil de todo, un estafador con un ánimo de lucro desmedido, la estafa como forma de vida, la actuación en connivencia con personas de su círculo de confianza, familiares o amigos cercanos y.... eso una persona muy controladora, muy ingeniosa y muy inteligente, porque para hacer todo esto y tener controlado todo hasta el último detalle de cualquier cosa hay que ser personas muy inteligentes, hay que reconocerlo que sí.

<sup>xxix</sup> el hacker no es una persona mala eso también que quede claro que lo que es el concepto hacker no es un delincuente o sea todo hacker no es delincuente. Osea son gente que está ávida de conocimientos quiere saber cosas están muy involucrados en el tema de la seguridad informática y les gusta descubrir diferentes fallos

<sup>xxx</sup> el concepto hacker no es siempre una persona mala. ¿Vale?

<sup>xxxi</sup> el fin siempre es económico.

<sup>xxxi</sup> Internet lo que está, y bueno ya está muy consolidada la creación de una comunidad pedófila una comunidad pedófila que les protege, que les da soporte, que les comprende, que les hace ver que lo que están haciendo no está mal.

<sup>xxxi</sup> que eso es una acción sexual más, que la sexualidad de los niños tiene que ser enseñada por un adulto y bueno que el amor entre adultos y niños es posible todas esas cuestiones que la sexualidad nace desde que se es bebé y que bueno pues que no es ninguna cosa grave el que se realicen actos sexuales con los menores.

<sup>xxxi</sup> tratan de justificarse a sí mismos como que el acto que están realizando es algo normal y es algo natural.

<sup>xxxi</sup> estoy jugando.

<sup>xxxi</sup> me echan a mí la culpa de todo lo que pasa pero es que el niño le dejaban ir desnudito por la casa.

<sup>xxxi</sup> ha entrado el crimen organizado en la producción de pornografía infantil, lo cual es gravísimo.

<sup>xxxi</sup> no tienes que ir buscándolo por ahí por la calle.

<sup>xxxi</sup> ¿Por qué quieren ver niños desnudos?, no lo entiendo, es para desquitarse del mono que provoca verlos en acción, ¿para qué estar viendo fotos de hace 30 años? Si puedes estar viendo fotos actuales, ustedes que sean niño adictos o que, se cree que por ser más lights, esas fotos no son ilegales, pues si que lo son. Quizás no tanto pero lo siguen siendo. Ala que os den mucho por culo.

<sup>xi</sup> NPEX2:No, él sabe que no está bien pero bueno lo ve como, yo creo que lo que nos decía es que, ah si, una cosa que decía es dice: no he matado a nadie, no soy asesino, no soy un traficante de drogas, o sea no veía como que esto era un delito o bajo su conciencia un delito grave, eso si que nos lo dijo, no soy un traficante de drogas, vale, yo pago por lo que he hecho pero joder, no entiendo porque esto es tan grave o esta pena tanto porque no soy, no he matado a nadie, no soy un traficante de drogas, no tenía una percepción de que es un delito violento sino que tenía esta percepción.

<sup>xi</sup> Pero que nunca hacíamos daño.

<sup>xlii</sup> podría haber accedido a más datos, no voy más allá.



---

<sup>xliii</sup> Sí, sabía que estaba cometiendo un acto ilícito pero lo veía como diciendo no tengo la sensación de que iba, que tampoco quería hacer más daño, yo quería mi dinero.

<sup>xliv</sup> es que quería comprarme una bicicleta.

<sup>xlv</sup> los que tenían entre 12 10 entre 10 y 13 años esos ya sí porque tampoco eran conscientes de que es lo que están haciendo, simplemente bueno, les van a dar 50 € les van a dar una PlayStation y ya stá no tiene ninguna importancia.

<sup>xlvi</sup> Estamos en crisis.

<sup>xlvii</sup> bueno pues cuando los detienes todos, no saben de qué hablas, no sabes que es lo que estás investigando, evidentemente ellos no han hecho nada, no, ellos no, no, sólo tienen un negocio lícito que les fue mal y que no muestran ningún tipo de arrepentimiento y no eso si no que no llegan a reconocer ni tan siquiera el daño que han hecho.

<sup>xlviii</sup> Evidentemente, él dijo que esto no era un delito que era un negocio lícito, que él era un empresario que daba trabajo a muchísima gente, que hacía la función social muy buena porque gracias a él había mucha gente trabajando.

<sup>xlix</sup> si eran de algún modo conscientes.

<sup>i</sup> Jorge: ¿Pero cómo una mentira para fuera o para si mismo?

NPEX1: No, una mentira para fuera, lo que pasa que en el momento esto es ilícito e ilegal se cae todo, o sea es que está reconociendo la existencia del delito.

<sup>ii</sup> La gente lo hace pues bueno, realmente, el cometer ese dicho “delito” está ahí a día de hoy no hay algo estipulado pero estaríamos robando o hackeando el coste de la Wi-Fi que supone mensualmente pongámosle 30/40 € ese tipo de delito pues bueno la gente dice Naaaaa esto no es nada y lo hago y a veces por el simple hecho de Qque bueno soy que he hackeado la Wi-Fi del vecino.

<sup>iii</sup> Primero yo creo, uno es por una motivación (pensando) por una ideología. El primero de todos es porque piensa en que puede cambiar, o sea el discurso este de “Anonymous”, el discurso este hacktivista de que podemos cambiar el mundo, fuera los corruptos, de que libertad a la hora de compartir información, o sea el discurso hacktivista este de “Anonymous” que estas totalmente integrado y que dices yo quiero colaborar a la causa, somos muchos que queremos cambiar el mundo, que tal. Entonces yo con mis conocimientos, lo poco que se lo que puedo poner en estos servidores pues lo voy a poner, hay un componente ideológico.

<sup>liii</sup> No, no si son ellas las que provocaban si, es constante también el groomer.

<sup>liv</sup> Jorge: O sea los groomers incluso también os han dicho que es culpa de las chavalas o chavales involucrados.

NPEX3: Sí, sí en muchas ocasiones.

<sup>lv</sup> no veía a la víctima.

<sup>lvi</sup> Jorge: ¿Y por qué crees que los más adultos sí que exigían ser ellos los que penetraban pero no se penetrados? Es decir, ¿Por qué se produce esa contradicción?

GCEX: Porque como estas agresiones son de carácter homosexual, el concepto que tiene el menor es que yo no soy homosexual. El momento en que yo no soy penetrado o yo no realiza nada, osea yo esto lo hago por dinero, es consciente de que está penetrando aun hombre adulto, ¿Vale? Pero su manera de pensar es decir yo no soy homosexual. ¿Sabes?

---

<sup>lvii</sup> Jorge: Y él, “Camaleón”, ¿llegasteis a saber de sus justificaciones, por qué lo hacía, por qué no? él ¿dijo algo al respecto, dejó entrever algo al respecto?

NPEX3: no, es que las motivaciones, realmente no las explicita excepto que se sientan culpables, ellos no, en principio no se siente culpable,.

<sup>lviii</sup> NPEX3: Esta persona, yo le tome declaración y lo negaba todo. Ni enseñándole las pruebas ni demás, todo lo negó completamente todo, siempre.

Jorge: ¿Pero qué no lo había hecho? ¿Que no era él?

NPEX3: Que no era él, que él no había hecho nada. Pero vamos, ya te digo, es que encontramos en su casa todo el material, hasta los consoladores que obligaba meterse a la niña de 6 años.

<sup>lix</sup> se cierra en banda y no.

<sup>lx</sup> tampoco, reconoce que son delito evidentemente pero, no justifica.

<sup>lxi</sup> no mostró resistencia pero tampoco colaboración.

<sup>lxii</sup> vale, yo sé lo que he hecho. Si han llegado hasta mi casa es porque tiene que haber pruebas más que suficientes para que hayan llegado hasta aquí, pero ahora es la guardia civil la que tiene que encontrar todos los indicios para demostrar lo que yo he cometido.

<sup>lxiii</sup> No te van a decir ni cuál es el origen de los beneficios económicos que han tenido, no te van a revelar quienes son sus clientes, no te van a revelar quienes son sus proveedores.

<sup>lxiv</sup> Percepción de seguridad.

<sup>lxv</sup> un grandísimo hijo de puta.

<sup>lxvi</sup> Siempre ponerse en el lugar del otro.

<sup>lxvii</sup> Por eso muchas personas, podemos contar anécdotas de que nos llamaban por ejemplo por teléfono y contaban, que joder yo es que pagaba la multa sin ningún tipo de problemas. Bueno, bueno, si, si es verdad pero yo creo que no es delito ver pornografía.

<sup>lxviii</sup> No, no yo en ningún momento he visto pornografía infantil he visto el video tal y el video tal de tal página web que es pornografía adulta y tal pero yo no se porque me sale esto de pornografía infantil, pero que si hay que pagar 100 euros que es lo de menos, que yo pago 100 euros.

<sup>lxix</sup> los padres eran de un estrato social medio-bajo. Vale, no vamos a decir que eran, o sea que vivían en osea vivían en una casa y en un barrio humilde pero que no era dentro de no eran chabolas, no eran vale osea era un estrato medio-bajo pero no bajo del todo.

<sup>lxx</sup> muchas trabas a la gente de abajo se ponen muchos candados.

<sup>lxxi</sup> Que no es lo mismo, pero bueno, la cultura de los gratis y de lo que bueno he conseguido y no me he gastado nada, y que bueno, estamos en crisis [...]no tiene conocimiento de toda la industria que va detrás del copyright, de los derechos de autor.

<sup>lxxii</sup> una PlayStation 3, ya sea te doy un teléfono móvil de última generación que vale 200 €, 300 €, 400 €.

<sup>lxxiii</sup> tenemos mejor tiempo, tenemos el sol, tenemos otras circunstancias que bueno que también nos ayudan a relacionarnos con la gente

---

<sup>lxxiv</sup> Pues es un mensaje redactado en palabras sudamericanas, incluso la cuenta de correo electrónico es de un dominio de @bolivia.com, que por el acento el ataque que ha sufrido es por parte de un sudamericano.

<sup>lxxv</sup> ¿por qué pides solo 2500 euros?. No porque es que quería comprarme una bicicleta.

<sup>lxxvi</sup> a día de hoy el valor que se la da a mantener una relación sexual no, osea un niño no la tiene muy clara que valor tiene ni cuanto puede costar.

<sup>lxxvii</sup> un ánimo desmedido de lucro.

<sup>lxxviii</sup> si yo quiero ganar dinero y no tengo escrúpulos.

<sup>lxxix</sup> todo se compra, hoy en día se compra absolutamente todo.

<sup>lxxx</sup> NPEX3: Sí, sí. Cada vez hay más mujeres en relación a esto y la mayoría de las que teníamos al principio de las mujeres que estaban en estos temas de pornografía infantil era evidentemente dentro de ámbito de prostitución, es decir como una forma más de ganar más dinero, pero también ahora estamos viendo que efectivamente también hay un grupo de personas que son mujeres y que son pedófilas que son pederastas.

<sup>lxxxi</sup> hay mucha producción de pornografía infantil que solamente busca el interés económico, cuando hablamos de crimen organizado la captación de menores, la creación de web, el blanqueo de dinero procedente de la venta de la pornografía infantil estamos hablando ya de personas que no creen en ninguna cosa de esas, son intereses meramente económicos porque les produce mucho beneficio.

<sup>lxxxii</sup> Jorge: ¿Y en el tema por ejemplo de descargas, descargas de series, películas, música... Crees que la gente es consciente en este caso de que puede ser delictivo, crees que las personas piensan en algunos casos que es algo moral o inmoral? ¿Cuál es tu opinión al respecto?

PSEX: Mi opinión es que la gente, si puede conseguir algo gratis ¿para qué va a pagarlo?

<sup>lxxxiii</sup> Pongamos el ejemplo, si voy al cine y tengo que gastarme 8 € por ir al cine, por un entrada, si yo cojo y le doy con un simple click, encima estoy en mi casa, me pongo yo las palomitas y la Coca-Cola y me sale gratis... Que no es lo mismo, pero bueno, la cultura de lo gratis y de lo que bueno he conseguido y no me he gastado nada, y que bueno, estamos en crisis. Es que la crisis se profundiza y la gente no se gasta tanto en...

<sup>lxxxiv</sup> no tiene conocimiento de toda la industria que va detrás del copyright, de los derechos de autor, etc.

<sup>lxxxv</sup> La gente lo hace pues bueno, realmente, el cometer ese dicho "delito" está ahí a día de hoy no hay algo estipulado pero estaríamos robando o hackeando el coste de la Wi-Fi que supone mensualmente pongámosle 30/40 € ese tipo de delito pues bueno la gente dice Naaaaa esto no es nada y lo hago y a veces por el simple hecho de que bueno soy que he hackeado la Wi-Fi del vecino.

<sup>lxxxvi</sup> NPEX1: ¿Por qué colgaba esos videos? Pues ¿por qué piensas tú que colgaba los videos?

Jorge: A mí se me ocurren muchas cosas, claro es que si te lo digo

ES que realmente no me lo he parado a pensar, yo de verdad pienso este tío es tonto. Un tío que es un niño, un niño de papa que lo que quiere es presumir de sus hazañas y que no piensa en las consecuencias de sus actos y mucho menos piensa que como no le pillan en ese momento haciendo las carreras pues ya a través de internet menos. Entonces no piensa en ningún momento que pueda ser delito ni que se esta jugando la vida de nadie ni nada, entonces ¿quién hace eso?. Una persona que es una persona arrogante que presume de lo que tiene que los canales de YouTube los utiliza pues para

---

eso para jactarse del dinero y de los coches y todo lo que tiene y de la gente que está a su alrededor, porque no dejaban de ser pobres críos de 18 años con dos neuronas.

<sup>lxxxvii</sup> es la forma de captar a los menores a través de las redes sociales se capta a los menores pero luego se les lleva a otro sitio, es decir se les lleva a que faciliten las imágenes y los vídeos, bien a través de Skype o a través de aplicaciones que permite una rápida comunicación.

<sup>lxxxviii</sup> Ellos no saben que lo que están haciendo es realmente un delito.

<sup>lxxxix</sup> El tema de la educación existe una gran barrera que es una, se llama brecha digital, en la cual no puedes inculcar a los menores sin haber inculcado anteriormente a los mayores.

<sup>xc</sup> Un padre le compra una Blackberry a un niño de 11 años desconociendo de que en la mano tiene un arma que puede cometer bueno puede cometer el suicidio de una niña la cual la están abusando.

<sup>xc i</sup> una sensación que no les iban a pillar.

<sup>xc ii</sup> Comunidad pedófila.

<sup>xc iii</sup> Que es algo que visita todo el mundo, pues páginas de pornografía infantil, perdón, de pornografía, no de pornografía infantil de pornografía.

<sup>xc iv</sup> En España, un 4% de los menores entre 10 y 16 años dice haberse hecho a sí mismos fotos o vídeos en una postura sexy (no necesariamente desnudos ni eróticas) utilizando el teléfono móvil.

<sup>xc v</sup> y vas a meter datos, denuncia por denuncia y te hace estos esquemas y te saca las relaciones.